

# **PERFORMANCE WORK STATEMENT**

**In Support Of**

**CLIENT AGENCY:**

**United States Department of Agriculture (USDA)  
National Information Technology Center (NITC)**

**PROJECT TITLE:**

**Information Technology Support**

**~~Original Version dated December 18, 2014~~**

**Revision 1 dated January 23, 2015**

## Table of Contents

1.	BACKGROUND .....	- 4 -
2.	OBJECTIVE .....	- 4 -
3.	SCOPE .....	- 5 -
4.	APPLICABLE DOCUMENTS.....	- 5 -
4.1.	Applicable Regulations and Documents .....	- 5 -
5.	TASK REQUIREMENTS .....	- 6 -
5.1.	Contract Line Item Numbers (CLINs) .....	- 6 -
6.	PERSONNEL .....	- 7 -
6.1.	General Requirements.....	- 7 -
6.2.	CLIN Specific Experience and Expertise .....	- 7 -
6.3.	Training.....	- 7 -
6.3.1.	Contractor Staff Training .....	- 7 -
6.3.2.	Seminars, Symposia, Or User Group Conferences .....	- 7 -
6.3.3.	Mandatory Government Training .....	- 7 -
6.4.	Personnel Retention and Recruitment.....	- 8 -
6.4.1.	Work Transition Plan.....	- 8 -
7.	QUALITY .....	- 8 -
7.1.	Quality Control .....	- 8 -
7.2.	Quality Assurance.....	- 9 -
8.	DELIVERABLES.....	- 9 -
8.1.	Contractor Submission.....	- 9 -
8.2.	Government Review .....	- 9 -
8.3.	Data and Deliverable Rights .....	- 9 -
8.4.	Transfer of Ownership .....	- 9 -
8.5.	Monthly Invoice.....	- 10 -
8.6.	Monthly Status Report .....	- 10 -
8.7.	Phase-In / Phase Out .....	- 10 -
8.7.1.	Phase-In Plan .....	- 10 -
8.7.2.	Phase Out Plan .....	- 11 -
8.8.	Deliverable Matrix .....	- 11 -
8.9.	Other Reporting Requirements .....	- 12 -
9.	PERFORMANCE .....	- 12 -
9.1.	General.....	- 12 -
9.2.	Kickoff Meeting.....	- 12 -
9.3.	Period of Performance .....	- 12 -
9.4.	Place of Performance. ....	- 12 -
9.4.1.	Applicability of Telework.....	- 13 -
9.4.2.	Travel .....	- 14 -
9.5.	Hours of Work .....	- 14 -
9.5.1.	Standard Duty Hours Support.....	- 14 -
9.5.1.1.	Normal Workday - (work hour category A) .....	- 15 -
9.5.1.2.	Staggered Workday - (work hour category B) .....	- 15 -
9.5.2.	Non-Standard Duty Hours Support.....	- 15 -
9.5.3.	Continuity of Operations (COOP)/Disaster Recovery (DR).....	- 15 -
9.5.4.	Holidays .....	- 16 -
9.5.5.	Government Administrative Leave Situations .....	- 16 -
10.	GOVERNMENT FURNISHED EQUIPMENT/INFORMATION/ACCESS .....	- 16 -

10.1.	General.....	- 16 -
10.2.	Property.....	- 16 -
10.2.1.	Facilities.....	- 16 -
10.2.2.	Equipment at Authorized On-Site Federal Work Locations .....	- 17 -
10.2.3.	Facilities and Equipment at Remote Work Locations.....	- 17 -
10.2.4.	Materials .....	- 17 -
10.2.5.	Validation of Government Furnished Items (GFI) and Equipment Inventory .....	- 17 -
10.3.	Use of Government Property .....	- 17 -
10.3.1.	Desk Telephones .....	- 17 -
10.3.2.	Mobile/Wireless Telephones and Smart Devices .....	- 17 -
10.3.3.	Mail/Postage .....	- 18 -
10.3.4.	Electronic Mail (E-mail) .....	- 18 -
10.3.5.	Copiers .....	- 18 -
10.3.6.	Fax Machines .....	- 18 -
10.3.7.	Computer and Internet .....	- 18 -
10.3.8.	Canvassing, Soliciting, or Selling .....	- 18 -
10.3.9.	Security Violations Using Government Equipment.....	- 18 -
10.4.	Government Vehicles.....	- 18 -
10.5.	Return of Government Property.....	- 18 -
10.6.	Conservation of Utilities .....	- 19 -
11.	SECURITY .....	- 19 -
11.1.	United States Citizenship.....	- 19 -
11.2.	Security Awareness Training .....	- 19 -
11.3.	Background Investigation Requirements .....	- 20 -
11.4.	Access to Sensitive/Critical Data.....	- 21 -
11.4.1.	Non-Disclosure Agreement.....	- 21 -
11.4.2.	Data Access.....	- 21 -
11.5.	Security Incident Reporting .....	- 21 -
11.6.	Permanent Security Badge Requirements.....	- 21 -
11.7.	Display of Permanent Security Badges.....	- 22 -
11.8.	Temporary Security Badge Requirements .....	- 22 -
11.9.	Facility Security Requirements.....	- 23 -
11.10.	Parking Requirements.....	- 24 -
12.	ADMINISTRATIVE CONSIDERATIONS.....	- 24 -
12.1.	Government Representatives .....	- 24 -
12.2.	Procedures for Payment .....	- 25 -
12.2.1.	Performance Based Payment Percentages .....	- 25 -
12.2.2.	Submission.....	- 25 -
12.2.3.	Non-Compliance .....	- 25 -
12.3.	Personal Service.....	- 25 -
12.4.	Section 508.....	- 25 -
12.5.	Privacy Act.....	- 25 -

## PERFORMANCE WORK STATEMENT (PWS)

### 1. BACKGROUND

The National Information Technology Center (NITC) within the Office of the Chief Information Officer (OCIO) is charged with offering cost competitive, cloud-based, automated data processing hosting services to USDA and other federal government organizations. The NITC generates operating revenue under a “fee-for-service(s)” model administered through USDA’s working capital fund. NITC has grown in responsibility as the number of physical and virtual, mid-tier servers has grown based on customer demand. It is anticipated that the growth will continue. At the time of preparing this performance work statement, the NITC is supporting USDA customers and other federal government organizations as they strive to achieve the President’s mandate to dispose of unneeded federal real estate and consolidate federal data centers.

The NITC provides comprehensive, cloud-based hosting services, associated operations, security, and professional support services to a customer base of 35 federal organizations. The Enterprise Data Center hosts business applications supporting millions of citizens across the United States of America. The NITC organization has been designated a USDA Enterprise Data Center with locations in Kansas City, MO; St. Louis, Missouri; Beltsville, Maryland; Washington, DC; Salt Lake City, UT; Fort Worth, TX; and Fort Collins, CO. The NITC has earned the title of a GSA FedRamp certified cloud service provider.

The NITC utilizes an IT Infrastructure Library / IT Service Management (ITIL/ITSM)-based framework to develop processes & policies for all work activity tracking, process management and workflow. The current ITSM automation suite is provided through BMC’s Remedy COTS offering. The ITSM suite will generate task assignment queues. The policies and direction for many of these automated processes are directed by the Enterprise Change Control Board (ECCB) which governs the tool implementation. The contractor shall use this tool and adapt to the methods implemented by the NITC. During the course of this task order, the ITSM Remedy systems of the NITC and International Technology Services (ITS) organizations will continue to data share to provide unified responsiveness. It is anticipated that data sharing and ticket assignment will continue to be enhanced in the coming years.

The NITC also partners with the ITS to provide hosting and network solutions for USDA’s Service Center Agencies (i.e., Farm Service Agency, Natural Resources and Conservation Service and Rural Development). This task order seeks to continue to improve those services that are provided through the use of Memorandum of Understandings (MOUs), Service Level Agreements (SLAs) and Operating Level Agreements (OLAs). The contractor shall to adhere to the language and conditions of these documents. Copies of all MOUs/SLAs/OLAs relevant to this task order that are in place at the time of award will be provided to the contractor. The MOUs/SLAs/OLAs facilitate the understanding of the separate but shared roles and responsibilities for services that are provided by the OCIO organizations.

### 2. OBJECTIVE

The objective of this task order is to provide Information Technology (IT) support services to complement in-house capabilities in order to meet the short and long-range plans of both USDA and non-USDA serviced agencies. Specific objectives include, but are not limited to, those identified below.

- **Objective 1** - The Contractor shall work as a part of the technical support team that the NITC leverages to provide world-class data center service offerings and professional services to the USDA and other federal government customers (i.e., customer base) and shall enable the increased visibility of NITC value-added benefits by meeting or exceeding service expectations. In the data center operational support context, the support team is comprised of vendor-dispatched hardware maintenance personnel; vendor specific hardware and software technical “hot-line” support personnel; federal employees, and contractor employees. Given the complexity of the data center hosting environment and the customer base’s application software systems running on the hosting environment, system outages could require all or some of the support team, described above, to be mobilized to resolve the emergency.
- **Objective 2** - The Contractor shall support NITC data center officials in the completion of task assignments securing the availability, reliability and integrity of the data center through routine

operations & maintenance activities.

- **Objective 3** - The Contractor shall support NITC data center officials in the completion of work order priorities assigned through the ticketing system (i.e., NITC's implementation of BMC's Remedy COTS) and defined by the NITC Incident Management Process Guide. The contractor shall support incident, change and problem management and shall reinforce incident coordination and service metric tracking to staff.
- **Objective 4** - The Contractor shall support NITC data center officials in the preparation of documentation for the NITC Change Control Board.
- **Objective 5** - The Contractor shall support NITC data center officials with the implementation of federal mandates and the seam-less coordination with other OCIO organizational units.
- **Objective 6** - The Contractor shall support NITC data center officials with a full range of back office functions for the budgetary, financial and administrative management of the center.
- **Objective 7** - The contractor shall ensure close coordination, communication, and resource sharing and shall support resolution, restoration, and root cause analysis to reduce mean time to repair and reduce the overall cost of operations and maintenance support.
- **Objective 8** - The contractor shall support the achievement of long-term cost reduction by adapting ITIL best practices and applying automation to data center operations that reduce overall costs and better allocate resources.

### 3. SCOPE

The projects of the data center are national in scope and impact the United States economy. The scope of work for this PWS will cover a full range of functional areas and technical skill sets required to support the USDA, OCIO, NITC. The task order may include, but not be limited to, the IT support services for work to be accomplished using different computing environments that can include various hardware platforms, software, and telecommunications capabilities currently installed or planned to be installed by the NITC or customer agencies. This will require qualified personnel with expertise in computer equipment, software, and telecommunications facilities used in customer agency offices. The skill sets needed will vary depending upon the requirements.

USDA agencies are currently using, but are not limited to, the following types of hardware and software:

- NITC hardware and software include installed IBM-compatible mainframe computers, z/OS operating system with JES2 and VTAM, TSO, CICS, FOCUS, IDMS, and DB2.
- Other equipment currently in use includes SUN, HP, RISC based systems, and IBM-compatible PCs.
- Software currently in use includes ORACLE, S2K, SYBASE, C, SAS, COBOL, FORTRAN, UNIX, WINDOWS (200X), INFORMIX, DB2, Cold Fusion, Java, MS SQL, Adobe Acrobat, Adobe Photoshop, and Web Trends and other Web development tools, including WebSphere.

NITC supports multiple mainframe systems, several thousand mid-range systems, and various storage platforms. The current system environment includes: IBM, Sun, HP, and Intel-based servers with LINUX, AIX, Unix, HP-UX, Sun Solaris, Windows (9X, NT, and 200x), and Windows Data Center Operating systems, and storage solutions including Storage Area Networks. NITC offers multi-platform application, database support, and maintenance. Some of these include: High Availability Solutions, Mail/Directory Server Applications, Web Servers, and Database Applications.

*NOTE: The above information is for general reference and subject to change. The IT environments at the NITC and customer agencies are dynamic and can change constantly.*

### 4. APPLICABLE DOCUMENTS

#### ***4.1. Applicable Regulations and Documents***

The following documents (versions current at time of award) are incorporated into the resultant task order award. Succeeding revisions may be substituted or incorporated as required. This list is not all inclusive and or limited to the following:

- [http://wiki.edc.usda.gov/mediawiki/index.php/Main\\_Page](http://wiki.edc.usda.gov/mediawiki/index.php/Main_Page).
- ACM-0015-01 - Human Resources Management Contractor In-Process Rev 2 (PWS Attachment D-1).
- ACM-0015-02 - Human Resources Management Contractor Exit Process Rev 2 (PWS Attachment D-2).
- Applicable NITC Directives that will be released after the resultant task order award.

## 5. TASK REQUIREMENTS

The contractor shall furnish all personnel, services, and supervision to perform the requirements of this task order. The contractor shall provide facilities and equipment for back office administration. Contractor employees shall clearly identify themselves as such at all times (badge display; identification announcement prior to or at the commencement of meetings and teleconferences; and correspondence including e-mail, etc.)

### 5.1. Contract Line Item Numbers (CLINs)

The specific task requirements to be completed under the below identified CLINs are included in PWS Attachment A, which includes the performance standards for the firm fixed price (FFP) CLINs. Additional performance standards for the labor hour (LH) CLINs are included in PWS Attachment B. Additional CLIN specific requirement information, presented in a summary display, is identified in PWS Attachment C.

CLIN Number	CLIN Title	CLIN Type
001	Audit Support Services	FFP
002	Budget Analysis Support Services	FFP
003	Business Continuity Planning Services	FFP
004	Enterprise IT Services Portfolio Management	FFP
005	Facilities Operations Services	FFP
006	Information Systems Security Support Services	FFP
007	ITSM Process Development and Documentation Services	FFP
008	ITSM Service Asset and Configuration Management Support Services	FFP
009	Program/Project Management Review Support Services	FFP
010	Task Order Management	FFP
011	Technical Architecture Support Services	FFP
012	Technical Writer	FFP
013	ADDM Administration & Modeling Services	LH
014	Application Integration Engineering Support Services	LH
015	Data Center Hardware Support Services	LH
016	Database Administration Services	LH
017	Mainframe Systems Programming Services	LH
018	Network Engineering Services	LH
019	Remedy Engineering and Administration Services	LH
020	Security Administration Services - AD & Identity Management	LH
021	Security Administration Services - MF Auth., Role Mgmt. & Access Cont.	LH
022	Security Engineering - Assessment Services	LH
023	Security Engineering - Monitoring, Detecting & Analysis Services	LH
024	Security Engineering - Network Access Control Services	LH
025	Senior Application Engineering Services	LH
026	Server Automation Tool Support Services	LH
027	Storage Administration Services	LH
028	Systems Administration Services	LH
029	Systems Monitoring Administration Services	LH

## **6. PERSONNEL**

### ***6.1. General Requirements***

All contractor employees shall meet the minimum general requirements listed below.

- Strong written and oral communication skills in the English language. All contractor employees must be able to read, write, speak and understand English.
- Contractor personnel performing in a leadership capacity shall be capable of directing contractor personnel and interfacing with the Government and customers.
- Exceptional customer service skills.
- Strong time-management and prioritization skills.
- Ability to communicate applicable technical subject matter expertise to management and others.
- NITC follows the IT Infrastructure Library (ITIL) service operation best practices. It is important for the employees to demonstrate experience based on ITIL framework:
  - ITIL v3 foundation knowledge (or certification).
  - Ability to apply and provide feedback on service operation model and practices.

### ***6.2. CLIN Specific Experience and Expertise***

Documented experience and ability to demonstrate knowledge/skills/abilities with the required items (i.e. technologies, organizations, systems, processes, etc.) listed in the CLIN descriptions is required.

### ***6.3. Training***

#### **6.3.1. Contractor Staff Training**

The Contractor shall provide fully trained and experienced support staff for performance of the task order. Training of contractor personnel shall be performed at the Contractor's expense, except when the Government changes the requirements during performance of an on-going task and it is determined to be in the best interest of the Government. This will be negotiated on a case-by-case basis. Training at Government expense will not be authorized for replacement personnel nor for the purpose of keeping Contractor personnel abreast of advances in the state-of-the-art, or for training Contractor employees on equipment, computer languages, and computer operating systems that are available in the commercial market.

#### **6.3.2. Seminars, Symposia, Or User Group Conferences**

The Government will not authorize training for contractor employees to attend seminars, symposia, or User Group Conferences unless certified by the Contractor that attendance is mandatory for the performance of the task order requirement. When seminars, symposiums or User Group Conferences are authorized in writing by the COR, the Government will reimburse the Contractor for labor hours. The Contractor shall be responsible for expenses associated with the training, including, but not limited to, tuition, travel and per diem. This will be negotiated on a case-by-case basis

#### **6.3.3. Mandatory Government Training**

Mandatory Government training shall be tracked and monitored through USDA's AgLearn system. A new contractor employee must complete security training before a log-on ID to USDA systems is issued. The contractor shall provide the information to the employee to review. The contractor will then proctor an exam that the contractor employee will complete and provide to the NITC COR. The NITC COR submits the exam to the NITC Federal Training Coordinator for exam grading. Once the contract employee passes the test they will be granted access to USDA systems, including AgLearn. If the employee is not successful in scoring a passing grade (70% or higher) on the first or second attempt, the contractor will be requested to submit a new candidate for the vacant position. Each contractor employee must complete annual training classes as mandated by USDA. The current mandatory courses include Security Awareness, Privacy Basics, and some positions require Role-Based Security training. These mandatory AgLearn courses can be completed through the AgLearn website free-of-charge. The COR shall notify the

contractor of the training requirements and will provide the tools to complete this training. All required courses must be completed by the required dates by all contract employees. Mandatory government training classes may be completed during work hours. It is the intent of USDA to provide 30 calendar days written notice of annual training requirements to the Contractor's Task Order Manager. The Task Order Manager will be responsible for notifying subordinate contractor employees. In the event the contractor does not receive 30 calendar day notice, the contractor is still required to complete the training by the specified date(s).

#### ***6.4. Personnel Retention and Recruitment***

The Contractor shall make every effort to retain personnel in order to ensure continuity until contract completion. If it should become necessary to substitute or replace personnel, the Contractor shall immediately notify the COR in writing of any potential vacancies and shall submit the resume(s) of replacement personnel within 14 calendar days of the notification. Additionally, for all new positions identified by the Government, the Contractor shall submit the resume(s) of proposed personnel within 14 calendar days of the Government's initial request. The Contractor shall submit the resume(s) of all potential personnel selected to perform under this task order to the COR through Information Technology Solutions Shop (ITSS) for Government review and acceptance/rejection. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 calendar days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. Long-term absences are considered those longer than one week in duration.

##### **6.4.1. Work Transition Plan**

Due to the technical nature of the work and "least privilege" security access of user accounts, a situation could arise where work must be transitioned back to Government personnel upon a contract employee's departure from the workforce. In this situation, the contractor shall provide documentation in sufficient detail to allow for the transition of the workload to the Government. The Contractor shall provide documented processes that will serve as a basis for knowledge transfer and a historical record of the work accomplished. Documentation shall include a summary report on task requirements, contact information, and the location of documentation needed to provide continuity of service. This documentation must allow the Government to perform all tasks without the assistance of the Contractor.

## **7. QUALITY**

Both the contractor and Government have responsibilities for providing and ensuring quality services, respectively.

### ***7.1. Quality Control***

The contractor shall establish and maintain a complete Quality Control Plan (QCP) to ensure the requirements of this contract are provided as specified in accordance with the applicable Inspection of Services Clause. The CO will notify the contractor of acceptance or required modifications to the plan. The contractor shall make appropriate modifications (at no additional costs to the government) and obtain acceptance of the plan by the CO. The Government has the right to require revisions of the QCP (at no cost to the Government) should the incorporated plan fail to deliver the quality of the services provided at any time during the contract performance. The plan shall include, but is not limited to the following:

- A description of the inspection system covering all services listed.
- The specification of inspection frequency.
- The title of the individual(s) who shall perform the inspection and their organizational placement.
- A description of the methods for identifying, correcting, and preventing defects in the quality of service performed before the level becomes unacceptable.

On-site records of all inspections conducted by the Contractor are required. The format of the inspection record shall include, but is not limited to, the following:



- Date, time, and location of the inspection.
- A signature block for the person who performed the inspection.
- Rating of acceptable or unacceptable.
- Area designated for deficiencies noted and corrective action taken.
- Total number of inspections.

### ***7.2. Quality Assurance***

The Government will perform periodic reviews of the contractor's performance in accordance with the Government's Quality Assurance Surveillance Plan (QASP). The Government reserves the right to review services to be provided, including those developed or performed at the Contractor's facilities, to determine conformity with performance and technical requirements. Government quality assurance will be conducted on behalf of the CO. The COR will be appointed to coordinate the overall quality assurance of technical compliance.

## **8. DELIVERABLES**

Deliverables and due dates are identified in subsequent paragraphs.

### ***8.1. Contractor Submission***

Deliverables are to be transmitted with a cover letter, on the prime contractor's letterhead, describing the contents, electronically through GSA's web-based procurement system, ITSS, and to any other destination(s) as required per the Government's request. The contractor shall provide hard copy deliverables as required per the Government's request. All deliverables shall be produced using recommended software tools/versions as approved by the Government. All reports shall be accomplished utilizing the MS Office Software Suite to include MS Project as required.

### ***8.2. Government Review***

Government personnel will have 10 workdays to review deliverables (to include resubmissions) and provide written acceptance/rejection. The NITC USDA client representatives and/or the applicable COR(s) will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments, or provide rationale for not doing so within 5 days of receipt of comments. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a resubmission of the deliverable.

### ***8.3. Data and Deliverable Rights***

All information such as software, data, designs, test materials, documents, documentation, notes, records, software tools acquired, and/or software source code and modifications produced by the contractor under this PWS shall become the sole property of the U.S. Government, which shall have unlimited rights to all materials and determine the scope of publication and distribution. The contractor shall be required to deliver electronic copies of all documents, notes, records and software to the Government upon termination of the task order or expiration of the task order. The Government shall retain ownership of all proprietary information and intellectual property generated under this task order.

### ***8.4. Transfer of Ownership***

All data and documentation, including all studies, reports, spreadsheets, software, data, designs, presentations, documentation, etc., produced by the contractor or for the Government using this PWS are the property of the Government upon its taking possession of task deliverables or upon termination of the task order or expiration of the task order.

### ***8.5. Monthly Invoice***

The contractor shall provide a monthly invoice to be submitted simultaneously with the monthly status report. Both documents shall be provided to applicable parties. The invoice and monthly status report shall be submitted as a single file. The components of the single file shall be arranged in the following order: accounting format invoice, monthly status report, and additional documentation as required.

The invoice shall include but not be limited to:

- Labor hours expended. The labor hours expenditure information shall include the identification of the employee name, labor category, hourly labor rate, and total number of labor hours expended.
- Supplemental Accounting Code Information. The invoice shall include a supplemental electronic file that includes the name of each contractor employee, the number of hours worked in the month associated with the NITC accounting/shorthand code associated with the work performed. PWS Attachment E is provided for informational purposes.
- Supporting documentation for travel costs. Invoices including travel costs shall include supporting documentation as required by the Federal Travel Regulation (FTR) (receipts for all costs \$75.00 or greater). Invoice submissions including travel costs shall include completed travel expense sheets (i.e. travel voucher) for each trip for each employee.

### ***8.6. Monthly Status Report***

Monthly status reports shall include, but is not limited to, the items identified below.

- Status of task directives, schedules, deliverables. Status of task directives shall include a summary description and schedule of all task directives completed during the reporting period, all task directives currently on-going during the reporting period and all known task directives assigned for future reporting periods.
- current and cumulative task funding status (direct labor and travel funding status to be reported separately as required),
- outstanding issues, and proposed resolution approaches and actions to resolve any outstanding issues.
- Staffing report identifying current staffing roster, all current vacancies, and a record of all staffing departures
- Summary of the Scheduled Absence Calendar Availability deliverable for the two month period following the end of the MSR reporting period that clearly identifies and lists the scheduled absences
- Listing of all training to be completed within the two month period following the end of the MSR reporting period
- The monthly invoice shall be submitted simultaneously with the monthly status report.

### ***8.7. Phase-In / Phase Out***

#### **8.7.1. Phase-In Plan**

The contractor may or may not propose a separately priced transition period, for a duration to be determined and proposed by the contractor, but shall not exceed a period of 30 calendar days. The transition period is defined as the period of time (during the Phase-In) when the new contractor and the incumbent contractor will both be providing support to the client as required to support the transition to the newly awarded task order. If the contractor chooses to propose a transition period, such period shall be included and addressed within the below identified Phase-In Plan.

The Contractor shall develop a Phase-In Plan. Such Phase-In Plan shall present a clear understanding of the Phase-In tasks required, the issues likely to result from non-incumbent Contractor performance, and the Contractor's proposal to resolve such issues. The Phase-In Plan shall include a clear and feasible strategy for delivering services required within the periods specified by the Plan and shall include a detailed plan-of-action and milestones to transition the functions identified in this PWS in a well-planned, orderly, and efficient manner. The Phase-In Plan shall include, at a minimum:

- Staffing plan.
- Development and submission of required deliverables.
- Interface with the Government and incumbent contractor (if applicable) during Phase-In, to include meetings or status reports, as required.
- Approach to maintaining quality and minimizing disruption during Phase-In.
- Development and dissemination of operating instructions, procedures, and control directives.

#### 8.7.2. Phase Out Plan

During phase-out of this task order, which is determined to be a period of 90 days prior to the lifecycle end date of the task order, a smooth and orderly transition between the incumbent contractor and the successor contractor is necessary to ensure a minimum disruption to vital Government business. The Contractor shall cooperate to the extent required to permit an orderly changeover to the successor Contractor. The phase-out will be deemed completed by the COR when it is determined by the Government that the transition of property, data, and information developed as a part of this task order have been successfully changed over from the outgoing Contractor to the Government and the successor Contractor as required. Phase out activities include, but are not limited to, the tasks below.

- Submission of official comprehensive phase out plan.
- Daily communication of staffing status (i.e. projection of when incumbent contractor employees will off-board from the incumbent task order and identification of additional incumbent resources, such as a transition team, that may be needed to support the transition efforts) and overall phase out status, in accordance with the accepted phase out plan.
- Maintain the phase out schedule included within the phase out plan.
- Transition of property.
- Transition of supporting documentation.
- Transition of accounts (e.g. user accounts and user access).
- Knowledge transfer on the established installation, operation, and maintenance procedures of the technologies supported. The phase out plan shall clearly describe the proposed methodologies to be utilized for such transfer (e.g., written documentation, manuals, formal classroom type training, one-on-one training sessions, etc.).
- Execution and submission of phase out checklist, to include Government acceptance.

#### 8.8. Deliverable Matrix

Title	Description	Due Date
Quality Control Plan.	Refer to PWS paragraph 7.1.	Submission due concurrent with contractor quote. If requested, a final QCP shall be furnished for acceptance by the GSA Contracting Officer addressing any Government comments provided no later than 30 calendar days after task order award.
Monthly Invoice.	Refer to PWS paragraph 8.5.	The 15th calendar day of the month following the reporting period.
Monthly Status Report.	Refer to PWS paragraph 8.6.	The 15th calendar day of the month following the reporting period.
Phase-In Plan (Transition Plan).	Refer to PWS paragraph 8.7.1.	Submission due concurrent with contractor quote. If requested, a final plan shall be furnished for acceptance by the GSA Contracting Officer addressing any Government comments provided no later than 15 calendar days after task order award.
Phase Out Plan.	Refer to PWS paragraph 8.7.2.	120 calendar days prior to the period of performance end date.
Project Specific Deliverables.	Plans, Reviews, Assessments, Reports, etc.	To be determined at the time the project specific task directive is assigned to the

		contractor.
--	--	-------------

### ***8.9. Other Reporting Requirements***

In addition to the deliverable requirements identified above, the contractor shall comply with the following:

- The contractor shall bring problems or potential problems affecting performance to the attention of the COR as soon as possible. Verbal reports shall be followed up with written reports, when directed by the COR, within 24 hours.
- The contractor shall provide, in writing to the COR, the results of all meetings with the client that affect and/or change conditions or result in additional agreements or requirements. The contractor shall not perform any work outside the scope or requirements of this PWS and resultant order without express written approval of the CO.

## **9. PERFORMANCE**

### ***9.1. General***

Work is to be accomplished through the General Services Administration (GSA), Federal Acquisition Service (FAS), Great Lakes Region, through its task order with the contractor. Certification by the Government of satisfactory services provided is contingent upon the contractor performing in accordance with the terms and conditions of the referenced task order, this document, the approved technical and cost quotes, and all amendments. The client's representative, GSA's representatives, and the contractor's representative(s) shall meet when deemed necessary at the client's request. The client representative, the GSA representatives, and the contractor's representative may meet at the place determined by the client representative and GSA representatives.

### ***9.2. Kickoff Meeting***

Within 7 days of contract award, the Contractor shall initiate work on this task order by meeting with key client agency representatives, to include GSA, to ensure a common understanding of the requirements, expectations, and ultimate end products. The contractor shall discuss the overall understanding of the project and review the background information and materials provided by the client. Discussions will also include the scope of work, deliverables to be produced, how the efforts will be organized and project conducted; assumptions made/expected and results. A concerted effort shall be made to gain a thorough understanding of the client agency expectations. However, nothing discussed in this or in any subsequent meetings or discussions between the client and the Contractor shall be construed as adding, deleting, or modifying any task order requirements, including deliverable specifications and due dates.

### ***9.3. Period of Performance***

The anticipated period of performances are identified below. The actual periods may be adjusted based on the duration of the transition period, if applicable.

Transition Period:	June 1, 2015 through June 30, 2015 (maximum duration)
Base Year:	July 1, 2015 through June 30, 2016
Option Year 1:	July 1, 2016 through June 30, 2017
Option Year 2:	July 1, 2017 through June 30, 2018
Option Year 3:	July 1, 2018 through June 30, 2019
Option Year 4:	July 1, 2019 through May 31, 2020

### ***9.4. Place of Performance.***

The Primary Place of Performance shall be in NITC government facilities. When required by the Government, the Contractor shall also perform Task Order related activities at other Government and Contractor facilities within the local area. For the purposes of this Task Order, local area facilities are defined as those within 50 miles of a Primary Place of Performance. Reimbursement for local area travel shall not be authorized. Contractor requests for alternate performance locations (i.e. telework and work from other Government

facilities) will be reviewed and considered on a case-by-case basis. The contractor shall obtain the required authorization prior to performing work at an alternate performance location. A list of the authorized NITC work locations are listed below. The work locations are subject to change.

- a) Kansas City, Missouri (NITC-KC) Main Location:  
USDA National Information Technology Center  
8930 Ward Parkway  
Kansas City, Missouri 64114-3363
- b) St. Louis, Missouri Location at the Goodfellow Federal Complex:  
United States Department of Agriculture  
National Information Technology Center - STL  
Goodfellow Federal Complex  
4300 Goodfellow Blvd, Bldg. 104  
St. Louis, Missouri. 63120
- c) Washington, D.C. (NITC-DC) Location:  
USDA National Information Technology Center  
Room S-100, South Building  
1400 Independence Avenue, S.W.  
Washington D.C. 20250
- d) Ft. Collins, Colorado Location:  
USDA  
Building A  
2150 Centre Avenue  
Fort Collins, Colorado 80526
- e) George Washington Carver Center (GWCC), Maryland Location:  
USDA National Information Technology Center  
George Washington Carver Center  
5601 Sunnyside Ave.  
Beltsville, Maryland 20705-5000
- f) Salt Lake City, Utah Location:  
USDA-FSA-APFO  
2222 West 2300 South  
Salt Lake City, Utah 84119-2020
- g) Ft. Worth, Texas Location:  
Fort Worth Federal Center  
501 West Felix Street, Building 23  
Fort Worth, Texas 76115

#### **9.4.1. Applicability of Telework.**

All work performed at locations other than those identified as Government and/or contractor facilities shall be approved prior to performing the work. Federal contractors are not governed by Office of Personnel Management (OPM), GSA, or the individual agency policies; however, this does not prohibit contract employees from actually working at an alternate site, when/as appropriate **and specifically authorized by the Government.** Contractor shall develop telework policies to comply with the following requirements and address at a generic level within their Quality Control Plan. Alternate work arrangements for contractors shall be negotiated with the contractor's own employer and the appropriate agency official, to ensure policies and procedures are in close alignment and there is a clear and concise arrangement documenting the agreement. It remains the contractor's responsibility to ensure the services are performed

in accordance with the terms and conditions of the award. The following are applicable telework classifications included within PWS Attachment C:

- No – No telework available.
- Situational – Occasional, pre-arranged telework.
- Limited – Specified number of days per week for telework.

#### **9.4.1.1. Quality Control**

The contractor shall address the pertinent facts impacting performance and ensure all affected contractor resumes reflect the applicable work site. The contractor shall provide justification to the Government when identifying and submitting an individual as a telecommuter and address implementation processes and procedures within the quality control plan. The contractor shall be responsible for ensuring the Government has the required access/details necessary for the Government to perform quality assurance responsibilities.

#### **9.4.1.2. Compliance**

The contractor shall comply with all agency security telework policies. The contractor shall ensure all services provided from an alternate site comply with the Federal Information Security Management Act of 2002 (FISMA) and address the following, as a minimum:

- Controlling access to agency information and information systems;
- Protecting agency information (including personally identifiable information) and information systems;
- Limiting the introduction of vulnerabilities;
- Protecting information systems not under the control of the agency that are used for teleworking;
- Safeguarding wireless and other telecommunications capabilities that are used for teleworking; and
- Preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

#### **9.4.2. Travel**

The Contractor shall also perform non-local travel in support of this Task Order, as required by the Government. The COR, or the appointed representative, shall have sole authority to approve non-local travel requests necessary to support Task Order performance. Not later than 5 business days prior to the Contractor's estimated date of departure, the Contractor shall submit to the COR, via ITSS, a travel request, to include travel justification, the proposed itinerary, and cost estimates for such travel. Federal Travel Regulations apply. The Contractor shall be responsible for all travel arrangements including airline, hotel, and rental car reservations. The Contractor shall make every commercially reasonable effort to schedule travel far enough in advance to take advantage of reduced airfares.

### **9.5. Hours of Work**

The NITC is a shared services hosting provider (i.e., data center) that operates 24x7x365. Hours of support can and will be dependent on data center customer requirements for assigned tasks. The contractor shall coordinate work schedules with the COR to ensure service requirements are met, Government personnel are available, and customer results are achieved. The Contractor shall not exceed the monthly allocation of hours, calculated at 8 hours per day times the number of business days/month, without authorization from the COR. Additional details are provided below and the applicable work hour category for each CLIN is identified in PWS Attachment C.

#### **9.5.1. Standard Duty Hours Support**

The contractor shall provide for normal (during core business hours) and staggered standard duty hours support as required to ensure adequate coverage for US time zones.

#### **9.5.1.1. Normal Workday - (work hour category A)**

A standard normal workday is defined as any 8 hours of productive labor which must include the Core Business hours of 9:00 AM through 3:00 PM local time, Monday through Friday, excluding Federal Holidays. Exceptions may be required and shall be coordinated with the COR, to include short-term or long-term requirements for staggered workdays.

#### **9.5.1.2. Staggered Workday - (work hour category B)**

A standard staggered workday requires that on-site support shall be provided 6:00 AM through 6:00 PM local time, Monday through Friday, excluding Federal Holidays. Exceptions may be required and shall be coordinated with the COR, if coverage is required outside the 6:00 AM – 6:00 PM timeframe.

### **9.5.2. Non-Standard Duty Hours Support**

The contractor shall provide for scheduled (planned work hours) and un-scheduled (other than planned work hours), non-standard duty hours support as required. The contractor shall identify a primary and alternate point of contact for non-standard, un-scheduled duty hours requirements. To ensure the applicable labor hours allocations are not exceeded (typically 40 hours per week), labor hours expended in support of non-standard duty hours requirements shall be off-set by reducing the number of standard duty work hours by an equivalent number. **The off-set shall be completed within the same monthly reporting period, unless the non-standard duty work hours are expended in the last week of the monthly reporting period. Non-standard duty work hours expended within the last week of the monthly reporting period shall be off-set within the first two weeks of the following reporting period.**

#### **9.5.2.1. Scheduled (work hour category C)**

Scheduled non-standard duty hours support shall be coordinated with the authorized Government point of contact and the contractor's designated point of contact. Customers may request non-standard duty hours support for their environments (usually quarterly and during peak release or operational periods). Scheduled non-standard duty hours support may also be required to support a short term surge in requirements.

#### **9.5.2.2. Un-Scheduled (work hour category D)**

The Government may also request that the contractor provide un-scheduled (e.g., emergency technical support), non-standard duty hours support. The contractor shall respond within 15 minutes of notification. When off-site support can resolve the issue, the contractor's personnel shall begin immediately upon notification. The contractor shall assess the cause, determine the scope of the problem, advise the appropriate Government organization, provide an estimated restoration time, and identify and implement action for problem resolution. When required, on-site support shall begin within one hour of notification to the contractor's designated individual. This unscheduled support may include:

- Remote telephone support with the Government Technical Staff and/or customers.
- Remote support on GFE. Contractor employees may be equipped with GFE that enables remote data center access/log-on. The Government will not incur any costs associated with home-based WiFi or LAN access to the Internet.
- Onsite support.

### **9.5.3. Continuity of Operations (COOP)/Disaster Recovery (DR)**

The National Security Presidential Directive/NSPD-51/Homeland Security Presidential Directive/HSPD-20, National Continuity Policy, requires Federal departments and agencies to maintain a comprehensive and effective continuity capability, including a Continuity of Operations (COOP) program. The COOP program, which also includes pandemic preparedness, ensures the continuation of essential functions under emergency situations.

An emergency may require personnel to temporarily relocate to a pre-designated, alternate work site or telework to ensure continuity of essential functions. A contract position may support the NITC's COOP plan, and the contractor may be required to report for work to assist the NITC federal staff in supporting critical business functions following a formal disaster declaration. Contract employees, under this scenario, are required to deploy to the alternate work site within 12 hours of COOP Plan activation for the support of government identified essential functions. The deployment to the alternative work site may last for up to 30 days. Travel and per diem expenses, if required, will be reimbursed in accordance with the Federal Travel Regulation (FTR).

NITC will also engage in "PLANNED" Disaster Recovery Exercises throughout a given Fiscal Year. As these exercises are typically planned well in advance, NITC may require contract employees' participation in these exercises after appropriately coordinated advance notice. There may also be the limited possibility of an "UN-PLANNED" Disaster Recovery Exercise. Unplanned exercises are typically conducted during business hours and NITC may require contract employees' participation after immediate notice. Travel is not expected to be required during DR Exercises/testing.

#### **9.5.4. Holidays**

The contractor is hereby advised that government personnel observe the following holidays: New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas. In addition to the days designated as holidays, the government may observe the following days: any other days designated by Federal Statute; any other days designated by Executive Order; and any other days designated by the President's Proclamation. This includes Inauguration Day (Washington, D.C. metropolitan area only). Observance of such days by government personnel shall not be a reason for an additional period of performance, or entitlement of compensation. In the event the contractor's personnel work during the holiday, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost.

#### **9.5.5. Government Administrative Leave Situations**

When the agency grants administrative leave to its employees, on-site assigned contractor personnel may be dismissed by the contractor. The contractor agrees to continue to provide sufficient personnel to perform task orders already in operation or scheduled, and shall be guided by the instructions issued by the COR. The Government will not pay for the labor hours during the leave granted to contract personnel as a result of inclement weather, potentially hazardous conditions, explosions, and other special circumstances.

## **10. GOVERNMENT FURNISHED EQUIPMENT/INFORMATION/ACCESS**

### ***10.1. General***

The Government shall provide, without cost, the facilities, equipment, materials and services listed below. The Government furnished property and services provided as part of this task order shall be used only by the contractor only to perform under the terms of this task order. No expectation of personal privacy or ownership using any USDA electronic information or communication equipment shall be expected. All property at Government work sites, except for contractor personal items will be assumed to be government property unless an inventory of contractor property is submitted and approved by the CO/COR. Contractor personal items do not include computers, external drives, software, printers, and/or other office equipment (e.g., chairs, desks, file cabinets). The contractor shall maintain an accurate inventory of Government furnished property.

### ***10.2. Property***

#### **10.2.1. Facilities**

The Government will provide facilities at the authorized work locations specified in the task order. Use of the facilities by contractor employees will include all utilities, telephone, janitorial services and furniture for contractor employees performing tasks. The Government will provide the contractor access to buildings as required, subject to the contractor's employees obtaining the required security clearances.



#### **10.2.2. Equipment at Authorized On-Site Federal Work Locations**

The Government will provide the following at authorized on-site Federal work locations:

- a) A suitable work environment (i.e., telephone, office space and furniture).
- b) A personal computer/laptop and auxiliary hardware and software required in the performance of the task order.
- c) Network connectivity required to perform work assignments. Network and computer access rights commensurate with work assignments.
- d) Pagers, headsets, cell phones and maintenance agreements for such equipment when determined to be applicable by the COR. The Government will replace items that are determined to be beyond economical repair by the COR unless damage or loss is determined to be due to contractor negligence.

#### **10.2.3. Facilities and Equipment at Remote Work Locations**

When work from a remote location is authorized by the COR, the contractor will not be reimbursed for costs associated with remote connectivity from cell phones, WiFi access or Internet connection.

The contractor shall be responsible for ensuring the contractor employee has an adequate and safe office space that sufficiently protects Government equipment and information from loss, theft or unauthorized access. The contractor shall establish a telework agreement with the contract employee. The agreement, given a minimum of 24 hours of advanced notice, shall allow periodic inspections of the alternate work location can be undertaken. The purpose of the inspection is to ensure proper maintenance of Government-owned property and worksite conformance with safety standards and other specifications. The contractor is informed that telework is not a substitute for dependent care (i.e., child care or elder care) and that the appropriate arrangements must be made to accommodate children and adults who cannot care for themselves, while performing official duties of this contract at an alternate work location.

#### **10.2.4. Materials**

The Government shall furnish basic reference manuals, and any revisions, updates, and changes thereto for use by the contractor necessary to perform work assignments under the task order.

#### **10.2.5. Validation of Government Furnished Items (GFI) and Equipment Inventory**

The contractor shall develop and maintain a complete GFI inventory that shall be made available to the Government upon request. Within three (3) work days of receipt of any GFI, the contractor shall validate the accuracy of the materials and notify the COR, in writing, of any discrepancies.

NOTE: Validation shall consist of the Contractor checking for physical and logical completeness and accuracy. Physical completeness and accuracy shall be determined when all materials defined as Government furnished are provided, as defined in the task order. Logical completeness and accuracy shall be determined when all materials defined and associated with a program, system, or work package are provided.

### ***10.3. Use of Government Property***

#### **10.3.1. Desk Telephones**

Government telephones are provided for use in conducting official business. Contractor employees are permitted to make calls that are considered necessary and in the interest of the Government. The contractor will follow the same USDA and NITC policies as Government personnel the govern telephone usage.

#### **10.3.2. Mobile/Wireless Telephones and Smart Devices**

Government issued mobile/wireless telephone and smart devices may be assigned to contractor employees when the Government determines it is in the Government's best interest. Contractor employees are prohibited from using any Government issued device for personal use and would be subject to paragraph 10.3.9.

### **10.3.3. Mail/Postage**

Contractor employees shall not have their personal mail directed to Government offices or use Government-furnished postage for personal benefit. The contractor shall follow the same USDA and NITC policies as Government personnel that govern mail usage including overnight delivery.

### **10.3.4. Electronic Mail (E-mail)**

All Government e-mail access and use by contractor employees shall be in support of the individual's official duties and task responsibilities. All information that is created, transmitted, received, obtained, or accessed in any way or captured electronically using USDA's e-mail systems is the property of the Government. Contractor employees shall have clear identification in their e-mail signature block that identifies themselves as contractor employees in support of USDA NITC. Contractor employees are prohibited from forwarding e-mail generated from a Government provided e-mail account to personal mobile devices.

### **10.3.5. Copiers**

Copiers are to be used to copy material for official Government business only in the performance of the tasks in this task order.

### **10.3.6. Fax Machines**

Contractor employees shall not use fax machines for other than official Government business in the performance of the tasks in this task order.

### **10.3.7. Computer and Internet**

All Internet and electronic media access accomplished by contractor employees (utilizing Government furnished equipment) shall be for official Government business in the performance of the tasks in this task order.

### **10.3.8. Canvassing, Soliciting, or Selling**

Contractor employees shall not engage in private activities for personal gain or any other unauthorized purpose while on Government-owned or leased property, nor may Government time or equipment be utilized for these purposes.

### **10.3.9. Security Violations Using Government Equipment**

Any contractor violating USDA security policies, guidelines, procedures, or requirements while using Government equipment or while accessing the USDA network may, without notice, have their computer and network access terminated, be escorted from their work location, and have their physical access to their work location removed at the discretion of the CO/COR. The CO/COR will notify the contractor of the security violation and request immediate removal of the contract employee.

## ***10.4. Government Vehicles***

The use of Government-furnished vehicles is NOT authorized under this task order, **unless specific authorization is provided at the time of the proposed utilization**. If a vehicle is needed to perform required services, it must be supplied by the contractor for their employees' official government business needs. This paragraph is not applicable to rental vehicles utilized during approved travel under the contract.

## ***10.5. Return of Government Property***

All Government property, data, software, information, documentation and equipment whether furnished by the Government to the contractor, created by the contractor, or acquired by the contractor with Government funding is property of the Government and shall be delivered/transmitted to the COR upon termination or expiration of the task order or per instructions from the CO.

### ***10.6. Conservation of Utilities***

The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating practices that preclude the waste of utilities, which shall include:

- a) Lights shall be used only in areas where and when work is actually being performed.
- b) Mechanical equipment controls for heating, ventilation, and air conditioning system shall not be adjusted by the contractor or by contractor employees.
- c) Water faucets or valves shall be turned off after the required usage has been accomplished.

## **11. SECURITY**

USDA/OCIO has established legal and regulatory requirements that must be met before access is granted to federal IT resources. In order to gain access to USDA computer networks and computers, contractor personnel are required to initially complete the following requirements including, but not necessarily limited to:

- The USDA Information Security Awareness and Rules of Behavior training (web or paper-based). Additional and/or different courses may be required as USDA and NITC security policies change.
- The instructions to obtain USDA E-Gov access (eAuthentication).
- The documentation required for a security background investigation, which includes the Federal Bureau of Investigation's (FBI) National Criminal History Check ("fingerprint check") and eQIP.
- Information needed to obtain a Personal Identity Verification (PIV) card.

The contractor shall be responsible for ensuring compliance by its employees with all applicable federal regulations, to include those of GSA, NIST, USDA and HSPD-12. Contractors and their employees are subject to all Federal laws applicable to Government installations and are under the jurisdiction of the Federal Protective Service (FPS). The NITC COR, in conjunction with the USDA-OCIO Personnel Security Specialist (PSS), will ensure that the contractor submits the required Security Background Investigations/Clearances.

In addition, the contractor shall be responsible for ensuring compliance by its employees for any annual security training and reporting requirements of GSA, NIST, USDA and HSPD-12. Any contract employee working under this OCIO/NITC task order will be expected to follow the process for obtaining access to systems and notifying the Government for the termination of access upon the completion of performance under this task order. The contractor shall inform the COR and other designated NITC personnel if any changes are made in the status of contractor employees that would impact his/her access to USDA computer systems, and to follow the correct protocol for the creation, expansion and/or termination of such access.

### ***11.1. United States Citizenship***

No less than 75% of the contractor personnel assigned to this task, specifically to provide direct CLIN support, shall be United States citizens.

### ***11.2. Security Awareness Training***

Contract personnel who have access to USDA networks and computers will be required to take all security training necessary as determined by the Government to maintain access to the USDA network and computers. Currently, this includes an annual two hour or less, web-based Information Security Awareness training module and specialized training depending on the job function. The security training exam must be passed prior to any computer-system accesses are granted. Prior to an employee start-date, a paper-based exam must be administered by the contract site manager. If the employee is not successful in scoring a passing grade (70% or higher) on the first or second attempt, the contractor will be requested to submit a new candidate for the vacant position.

As USDA security policy changes, additional and/or different courses may be required. Contractor roles and permissions will be reviewed by the Government with the same frequency and at the same level as Government

employees. Access to Government facilities, networks, and computers will require contractors to follow all Government mandated security alerts, procedures, patches and upgrades.

### ***11.3. Background Investigation Requirements***

After proper submission of paperwork, the Government covers the costs of investigations and submits the investigation for processing of all required security investigations/clearances, unless identified differently within this section. The scope of the security/background check required and the forms to be completed shall be determined in accordance with the Common Identification Standard for U.S. Department of Agriculture Employees and Contractors, USDA Directive 4620-002. The Government sponsor for this process shall be the COR or Government representative appointed in writing by the CO. The contractor shall be responsible for the preparation and submittal of the required forms. The contractor personnel shall not be required or permitted to perform work prior to receipt of the required security approvals.

Prior to being engaged on this task order, the contractor's employee must first have been processed for a favorably adjudicated FBI fingerprint check. An unfavorable FBI fingerprint check will require that the contractor remove the employee from any further consideration pertaining to this task order.

The contractor should be aware of any of its employees possibly having had a background investigation through another government agency. The investigation, if verifiable by the Government and completed within the last 5 years, can be accepted by the Government in lieu of a FBI fingerprint check.

Fingerprinting Instructions: The COR will provide contact information to make arrangements for fingerprinting of the contractor employees. Fingerprinting instructions include:

- fingerprinting for Kansas City, MO based personnel can be accomplished by the Personnel Security Office (PSO) at 8930 Ward Parkway.
- fingerprinting for DC-based personnel can be accomplished by the PSO Assistant, at the USDA South Building or personnel at the Beltsville, Maryland data center; or,
- fingerprinting can be obtained from the local law enforcement agency after the PSO provides the fingerprint cards. The contractor shall pay for all costs of fingerprinting by local law enforcement agencies.

#### **Background Investigations:**

Assuming a prior favorable FBI fingerprint check has been verified, for taskings and task assignments that exceed 180 days in length, a full background investigation, processed through the Office of Personnel Management (OPM), will be required for all contract employees under this contract.

The background investigation, prior to being submitted to OPM, must be favorably reviewed at the local level by the PSO. The COR, working with the PSO, will determine what level of background investigation is required, based on the type and sensitivity of the duties and/or systems being accessed by the contractor. Current NITC policy requires processing of high-risk, public-trust investigations.

The Contractor is responsible for the immediate removal of employee(s) from the task order, if any person is identified as being a potential threat to the health, safety, security, general well-being, or operational mission of the USDA and its population. Additional items revealed in the background check that may be unacceptable are: conviction of a felony, a crime of violence or serious misdemeanor, a record of arrests for continuing offenses, adverse financial issues, or falsification of security documentation. As a reminder, an unfavorable FBI fingerprint check will eliminate a contractor's employee for further consideration under this task order. Additionally, if unfavorable information is noted on the security questionnaire or developed during the ongoing or final background investigation, the Government retains the right to have the employee immediately removed from the task order at the Government's discretion. Unless otherwise directed by the Contracting Officer, the contractor shall provide a replacement within ten (10) business days. New hires or substitute personnel are subject to the same security background requirements.

Special Procedures when the Data Center proper is the Primary Duty Station.

If a contractor's duty position at an NITC facility is located within the data center space, the additional provisions of NITC Directive A8 must be adhered to. Primarily, the contractor shall be required to have an investigation at the BI level. In addition to the favorable FBI Fingerprint check, the contractor must complete the online security questionnaire portion of the BI level investigation, which must then be favorably reviewed at the local level by the PSO's office. The online security questionnaire process must be initiated by the PSO and involves the use of the eQIP (Electronic Questionnaire for Investigation's Processing) system. Data center access cannot be approved until the online security questionnaire portion of eQIP has been completed, and the NITC Director or designee has approved the access.

#### ***11.4. Access to Sensitive/Critical Data***

Contractor access to data deemed sensitive and/or critical by the Government will follow guidelines set forth in FIPS Publication 199, USDA and NITC security policy and only following successful completion of all security training.

##### **11.4.1. Non-Disclosure Agreement.**

Due to the sensitive nature of the data and information being worked with on a daily basis, all Contractor personnel assigned to the Task Order are required to complete the Government provided non-disclosure agreement within 15 calendar days after Task Order award, or prior to task order assignment, to ensure information that is considered sensitive or proprietary is not compromised. Signed non-disclosure statements shall be provided to the COR.

##### **11.4.2. Data Access**

The contractor may be required to have access to live production data for the performance of this task order. Any records and data or information the contractor may have access to may be highly sensitive and confidential. The contractor shall not divulge or misuse any information about files, data processing activities or functions, user IDs or passwords, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. It is the contractor's responsibility to ensure that other persons have the proper authorization

#### ***11.5. Security Incident Reporting***

Contractors shall report the loss or suspected loss of equipment or paper-based data including Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII) information according to the NITC Incident Response Policy when the contractor or contractor's employee first becomes aware of the loss or suspected loss. If the contractor or contractor's employee does not have access to this procedure, then the incident should be immediately reported to the Agriculture Security Operations Center (ASOC) via the 24-hour Cyber Incidents Hotline, (866) 905-6890.

#### ***11.6. Permanent Security Badge Requirements***

A permanent security badge will not be issued until the security questionnaire has been completed and favorably reviewed. In order to gain access to NITC authorized work locations via a permanent security badge, all contractor employees are required to complete the Request for USDA Identification (ID) Badge, Form Number AD-1197 (Sept 2005). The contract employee will be given this form upon first arrival for duty by the Contractor. Form Number AD-1197 (Sept. 2005) requires two (2) forms of identification be submitted. Contract employees are required to provide this identification when first reporting for work. One form of identification must any one of items 1-4 in the list below (Primary ID). The other ID may be any of the forms of ID listed below (Primary or Secondary ID types).

##### **Acceptable Forms of ID:**

Primary Forms of Identification (Items 1-4)	
1. US Passport (unexpired or expired)	3. US Military ID card (unexpired)

2. Driver's license or ID card issues by a state or possession of the United States provided it contains a photograph (unexpired)	4. US Military Dependent's ID Card (unexpired)
Secondary Forms of Identification (Items 5-25)	
5. US Social Security Card issued by the Social Security Administration	16. Permanent Resident Card or Alien Registration Receipt card with photograph (Form I-151 or I-1551)
6. Original or certified copy of a birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal	17. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)
7. ID issued by federal, state, or local government agencies or entites, provided it contains a photograph.	18. Unexpired Temporary Resident Card (Form I-668)
8. School ID with photograph	19. Unexpired Employment Authorization Card (Form I-668A)
9. Voter's registration card	20. Unexpired Reentry Permit (Form I-327)
10. US Coast Guard Merchant Mariner card	21. Unexpired Refugee Travel Document (Form I-571)
11. Certificate of US Citizenship Form (Form N-560 or N-561)	22. Unexpired employment authorization document issued by DHS
12. Certificate of Naturalization (Form N-560 or N-570)	23. Unexpired Employment Authorization Document issued by DHS with photograph (Form I-668B)
13. US Citizen ID Card (Form I-197)	24. Driver's license issued by a Canadian Government Authority
14. Unexpired foreign passport with I-551 stamp or attached Form I-94 indicating unexpired employment authorization	25. Native American tribal document
15. ID card for use of Resident Citizen in the United States (Form I-179)	

### ***11.7. Display of Permanent Security Badges***

A permanent security badge must be worn at all times while in the facility. It must be displayed above the waist. The individual will retain possession of the permanent security badge as long as continued admittance to the site is needed. Ensuring the safekeeping, wearing, and visibility of Government furnished security badge is the responsibility of the person issued a USDA Identification (ID) Badge. A permanent security badge shall immediately be returned to the Government when the need for it ceases to exist.

### ***11.8. Temporary Security Badge Requirements***

The Contractor shall ensure that each of the contractor's employees has been issued a temporary badge while the Request for USDA Identification (ID) Badge, Form Number AD-1197 (Sept 2005) is being proceeded. Temporary or visitor badges will be provided for persons who are identified as having an infrequent or

temporary legitimate business need for access to the site. As noted above, tasks and task assignments that exceed 180 days will require a permanent badge. The temporary badge authorizes the wearer to enter and exit the secured areas where NITC workstations are located within applicable authorized work location. The badge must be worn at all times while in the facility. It must be displayed above the waist. The badge must be returned to the security desk at the close of the business day.

### ***11.9. Facility Security Requirements***

Due to NITC facility security policies, it is required that the facility guards be notified in advance of all visitors wanting to enter the facility. This 24-hour advanced notification must provide the names, dates, times, the nature of the visit and the visitor's point of contact (POC). All visitors must have a NITC POC in order to be admitted to the facility. Individuals arriving at the NITC data center facilities that do not provide a pre-arranged POC may be turned away.

- 8930 Ward Parkway Facility Visitors Entrance. The east lobby of the 8930 Ward Parkway facility is the entry point for all NITC visitors. Visitors shall check-in at the east lobby guard station, sign-in and be issued a visitor's badge. The visitor's POC will be notified of the visitor's arrival. The visitor will be screened by a hand-held magnetometer, and the visitor's belongings will be passed through an x-ray machine. Failure to voluntarily comply with these security measures will cause the visitor to be denied access to the facility. The visitor shall return all issued visitor's badges at the end of the day or upon leaving the facility for any reason. Point of Contact: PWS COR.
- St. Louis, Missouri Location at the Goodfellow Federal Center Complex. Entrance onto the Federal Center Complex is at the main gate accessible from Goodfellow Boulevard. The main gate is open 24/7 and manned by GSA security officers. All vehicles entering the Campus are required to have a permanent complex decal or a Federal Center Complex parking permit. This must be arranged with the point of contact before attempting to enter the Federal Center Complex. Visitors are required to undergo a vehicle inspection conducted by the guards at the gate. Visitors must sign in at the main entry and be on the entrance list prior to attempting to enter the Federal Center Complex. The visitor is issued a paper badge which is returned upon leaving the Complex. The visitor's point of contact (POC) is notified to come to the gate and escort the individual. The POC will coordinate the access requirements with the lead Agency, Rural Development. Point of Contact: Diego Maldonado, [Diego.Maldonado@ocio.usda.gov](mailto:Diego.Maldonado@ocio.usda.gov).
- Washington, D.C. (NITC-DC) Location. The COR must sponsor all contract employees into the Whitten-South Building Complex. To process a contractor for a site identification badge, the federal sponsor must submit a form to, Tawana Waller, the headquarters security contact for all Office of the Chief Information Officer organizations. Once the proper background checks and security process determined to be adjudicated acceptably, the contractor would report to Room 1408-South (1st floor, 4th wing) for photo identification badging. Point of Contact: Bryan Dixon, [Bryan.Dixon@ocio.usda.gov](mailto:Bryan.Dixon@ocio.usda.gov).
- George Washington Carver Center (GWCC), Beltsville, Maryland Location. The main entrance to the Carver Center is at Building 1. Building 1 has a 24x7 guard posted at the reception desk. Visitors check-in check at Building 1 reception desk, show a valid identification, sign-in and issued a visitor's badge and parking permit. The visitor's belongings are then passed through an x-ray machine. The visitor's POC will be notified of their arrival and escorted within the facility. Badging office is located in Building 1 just east of the reception desk. Point of Contact: Bryan Dixon, [Bryan.Dixon@ocio.usda.gov](mailto:Bryan.Dixon@ocio.usda.gov).
- Salt Lake City, Utah Location. The facility is open from 6am-6pm/Mountain time, Monday-Friday (closed Federal holidays). The facility is open to the general public. The public entry point is at the East side of the facility next to the flagpole. All general public are required to sign in, issued a temporary day-use visitor pass. Visitors needing access beyond the Customer Service Area need to be escorted by the POC. The visitor's POC will be notified of their arrival and escorted within the facility. Point of Contact: Lori Uhlhorn, [lori.uhlhorn@slc.usda.gov](mailto:lori.uhlhorn@slc.usda.gov); Denny Skiles, [denny.skiles@slc.usda.gov](mailto:denny.skiles@slc.usda.gov).
- Ft. Worth, Texas Location at the National Geospatial Center of Excellence with the Fort Worth Federal Center. The Fort Worth Federal Center entrance is at the main gate at 501 W. Felix Street. Boulevard.

The main gate is open 24/7 and manned by GSA security officers. Visitors are required to undergo a vehicle inspection conducted by the guards at the gate. The visitor's point of contact (POC) should be notified 24 hours in advance. The visitor's POC will be notified to come to the gate and escort the individual. The POC will coordinate the access requirements to Building 23 or 24, as applicable. Point of Contact: Paul Fukuhara, paul.fukuhara@ftw.usda.gov

- Ft. Collins, Colorado location at the Forest Services' Natural Resources Research Center, Building A, on the Colorado State University campus. The Natural Resources Research Center (NRRC) is located at 2150 Centre Avenue, Building A, Fort Collins, CO 80526. The main entrance is during normal business hours to visitors. The visitor's point of contact (POC) should be notified 24 hours in advance. The visitor's POC will be notified to come to the entrance and escort the individual. The POC will coordinate the access requirements to the building, as applicable. Point of Contact: Rick Rohlf, [rick.rohlf@ocio.usda.gov](mailto:rick.rohlf@ocio.usda.gov); Jordan Bancroft, (970-295-5710).

### ***11.10. Parking Requirements***

The contractor shall direct its employees to comply with applicable rules governing parking at each authorized work location. These rules may include the display of a parking permit in the windshield of a vehicle or the application of a parking permit to the exterior of a vehicle.

- 8930 Ward Parkway Facility Parking Requirements: The Contractor shall ensure that each contractor employee obtains a parking permit tag from the Government Security Staff. The tag shall be properly displayed and visible on any vehicle parked near the 8930 Ward Parkway physical plant. Vehicles only intermittently visiting the 8930 Ward Parkway facility shall park in the visitor parking area.
- St. Louis, Missouri Location at the Goodfellow Federal Complex: All vehicles on the Federal Center Complex grounds must have a permanent window decal or a Federal Center parking permit. Contact the St. Louis facility POC for arranging the appropriate vehicle pass.
- Washington, D.C. (NITC-DC) Location: There is no government provided parking available at this location.
- George Washington Carver Center (GWCC), Beltsville, Maryland Location: There is a separate parking area designated for visitors. USDA and contract employees from other locations are required to check in at the reception desk and get a temporary parking permit and park in employee parking area. Contact the GWCC POC for arranging the appropriate vehicle pass.
- Salt Lake City, Utah Location: The main parking lot is located East of the building with smaller lots located North and South of the main building. Contact the Salt Lake City for arranging the appropriate vehicle pass.
- Ft. Worth, Texas Location: From the guardhouse, proceed downhill, across the railroad tracks and take the second right. As you turn right you will go under Hemphill Street. Follow the street as it curves to the left. Yield at the sign, then cross the street into the parking lot on the east side of Building 23. Visitor parking is designated. Enter the building through the automatic doors under the blue awning. Contact the Fort Worth POC to arrange for a permanent vehicle pass.
- Ft. Collins, Colorado location: There are separate designated parking spaces for visitors. A temporary parking permit must be displayed on the dashboard of visitor vehicles. The temporary parking permit will be provided by the guard in Building A. Contact the Ft. Collins POC to arrange for a permanent vehicle pass.

## **12. ADMINISTRATIVE CONSIDERATIONS**

### ***12.1. Government Representatives***

GSA Contracting Officer's Representative  
Wendi Borrenpohl  
1710 Corporate Crossing, Ste. 3  
O'Fallon, IL 62269  
618.622.5806  
[wendi.borrenpohl@gsa.gov](mailto:wendi.borrenpohl@gsa.gov)



GSA Contracting Officer  
Yjuania Still  
1710 Corporate Crossing, Ste. 3  
O'Fallon, IL 62269  
618.622.5809  
[yjuania.still@gsa.gov](mailto:yjuania.still@gsa.gov)

Client Contracting Officer's Representative  
Carrie Coffman  
USDA, NITC, Resource Management Division (RMD)-RSSB  
8930 Ward Parkway  
Kansas City, MO 64114  
816.823.1249  
[carrie.coffman@ocio.usda.gov](mailto:carrie.coffman@ocio.usda.gov)

## ***12.2. Procedures for Payment***

### **12.2.1. Performance Based Payment Percentages**

The performance objectives and respective payment percentages based on relative importance to total task performance are identified in the CLIN descriptions contained in PWS Attachment A. This document also identifies the Government's proposed surveillance assurance methodology.

### **12.2.2. Submission**

Invoices are due no later than the 15<sup>th</sup> calendar day of the month following the reporting period. The contractor shall submit the invoices and supporting documents, through ITSS simultaneously with the MSR (as an acceptance item) to allow the client and the COR to electronically accept and certify services received by the client representative. The contractor is authorized to invoice only for the services and travel ordered by GSA and provided in direct support of the task order.

### **12.2.3. Non-Compliance**

Failure to comply with the procedures outlined may result in payment being delayed at no additional cost to the Government.

## ***12.3. Personal Service***

The client determined that use of the GSA requirements contract to satisfy this requirement is in the best interest of the Government, economic and other factors considered, and this task order is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled "Personal Services Contract". The Contractor agrees that this is a non-personal services task order. The Contractor is not, nor shall it hold itself out, to be an agent or partner of, or joint venture with, the Government. The Contractor agrees that his/her personnel shall neither supervise nor accept supervision from Government employees.

## ***12.4. Section 508***

All services and products provided in response to the requirements identified in this document shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and IT (EIT) Accessibility Standards (36 CFR part 1194).

## ***12.5. Privacy Act***

Work under this task order requires that personnel have access to Privacy Information. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable USDA rules and regulations.

## CLIN 001 - AUDIT SUPPORT SERVICES

### 1. OVERVIEW

The Security Governance Branch, within the Security Division, is responsible for policies, controls and plans which ensure that risks are managed appropriately. The branch provides strategic direction, ensures that objectives are achieved, and verifies that the enterprise's resources are used responsibly and are consistent with applicable Federal laws and regulations. The Branch is made up of three teams: Contingency Planning, Risk Management, and Internal Audit.

The objective is to obtain technical support for two of the Internal Audit Team's (IAT) missions: (1) performing the continuous assessment tasks of the USDA's Continuous Assessment and Authorization (A&A) process of the USDA Six Step Risk Management Framework (RMF) Process<sup>1</sup>, and (2) annual A-123 testing. The contractor may be required to make contacts with NITC customers, technical staff, business partners, managers, and internal and external auditors.

### 2. SCOPE/DUTIES

a) The scope covers the systems listed in the NITC Systems table below.

System Name	Acronym	System Type	Assessment Type
NITC Enterprise Services	ES	General Support System	Cont. Assess.
NITC Auxiliary Support System	AXS	General Support System	Cont. Assess.
NITC Customer Billing System	CIMS	Major Application	Cont. Assess. A-123
NITC Data Center	NITC Data Center	Site	Cont. Assess. A-123*
NITC Internal Services	NIS	Site	Cont. Assess. A-123*
NITC ITSM Services Environment	ISE	Major Application	Cont. Assess.
NITC Mainframe	NITC Mainframe	General Support System	Cont. Assess. A-123
NITC Management Support System	MSS	Minor Application	Cont. Assess.
NITC Midrange Systems	NITC Midrange	General Support System	Cont. Assess. A-123
NITC Telecommunications Network GSS	NITC Network	General Support System	Cont. Assess. A-123*
NITC Infrastructure GSS	NITC IaaS	General Support System	Cont. Assess

b) For the systems listed as "Cont. Assess." (Continuous Assessment), the contractor shall perform the continuous assessment tasks of continuous assessment and authorization (A&A) process following Step 6 of the RMF process (Step 6 of the RMF process mirrors Step 4 with the exception of the number of controls to be assessed). The controls to be assessed in Step 6 of the RMF process are determined by the current version of [Appendix E - Security Controls Assessment List and potentially other controls defined within the boundary of each system that may not be within the scope of Appendix E](#). The A&A process requires annual testing of approximately one-third of the controls with

<sup>1</sup> [The current version of USDA Six Step Risk Management Framework Process \(RMF\) Guide](#)

100% of the controls tested within a three year cycle. These tasks include, but are not limited to:

- i. Develop and document the Security Assessment Plan (SAP).
  - ii. Execute accepted SAP and assess the required Security Controls.
  - iii. Develop security assessment reports and recommend Plans of Action and Milestones (POA&M).
  - iv. Upon completion of the above tasks (identified as i, ii and iii), manage the process of completing the Step 6 Concurrency Review.
- c) For the systems listed in the NITC Systems Table as “Cont. Assess. A-123”, the contractor shall perform the A-123 assessment of the NITC systems according to the guidance provided by the USDA Office of Chief Financial Officer (OCFO) Senior Assessment Team (SAT). The tasks to be completed, according to OCFO SAT guidelines, include:
  - i. Develop and document the Test Plan.
  - ii. Execute General Computer Controls (GCC) testing in accordance with accepted test plan.
  - iii. Document Testing Results in Cyber Security Assessment Manager (CSAM).
  - iv. Develop the following reports and documentation: security assessment reports; Corrective Action Plans (CAPs) with recommendations, and the Summary of Aggregated Deficiencies (SAD).
  - v. Recommend Plans of Action and Milestones (POA&Ms).
  - vi. Draft Annual Certification Statements.
- d) For the systems listed in the NITC Systems Table as “Cont. Assess. A-123\*”, the contractor shall perform the assessment of specific A-123 controls the system provides, according to the guidance provided by the USDA Office of Chief Financial Officer (OCFO) Senior Assessment Team (SAT).
- e) The contractor shall update assessments when revisions to National Institute of Standards and Technology Special Publication (NIST SP) 800-53, and other applicable regulations and guidance, are adopted by the agency.
- f) Develop and execute a project plan(s) that defines responsibilities, timelines, deliverables, risks, and milestones necessary to accomplish the stated objectives.
- g) Provide a weekly project status report, orally and in writing.

### **3. EXPERIENCE AND EXPERTISE REQUIREMENTS**

- a) Working knowledge of the technical requirements of applying the Risk Management Framework to Federal information systems in an enterprise Federal data center.
- b) Working knowledge of the technical requirements of performing OMB Circular No. A-123 assessments to Federal information systems in a large Federal data center.
- c) Working knowledge of the technical requirements of applying the Federal Risk and Authorization Management Program (FedRAMP) requirements to Federal information systems in a large Federal data center.
- d) Proficient using MS-Word, MS-Excel and MS-Project software, and possess strong abilities in writing technical documents. Skilled in facilitating meetings.

#### 4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Continuous Assessment Tasks	<ul style="list-style-type: none"> <li>100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant all with applicable governing regulations, policies, directives and guidance.</li> <li>100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 6 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
A-123	<ul style="list-style-type: none"> <li>100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant all with applicable governing regulations, policies, directives and guidance.</li> <li>100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 6 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input

Project Planning and Management	<ul style="list-style-type: none"> <li>▪ The contractor shall develop, document, and maintain project plans 100% compliant with federal governing regulations, policies, directives, guidance and industry practice.</li> <li>▪ 100% of project plans shall include the identification of applicable responsibilities, timelines, deliverables, risks, milestones and other elements as required.</li> <li>▪ 100% of plan schedules and activities shall be coordinated with all required participants.</li> <li>▪ All issues impacting project schedules shall be communicated to government staff within one business day after determination of impact.</li> <li>▪ 100% of project plans shall be updated weekly.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 6 violations per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Weekly Status Report	<ul style="list-style-type: none"> <li>▪ 100% complete.</li> <li>▪ 100% accurate.</li> <li>▪ Submitted no later than (NLT) 2<sup>nd</sup> business day of the calendar week following the reporting period.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 1 violation per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Inquiry Response	<ul style="list-style-type: none"> <li>▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 6 violations per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input

Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input
---	--	--	--	------------------------------

## **CLIN 002 - BUDGET ANALYSIS SUPPORT SERVICES**

### **1. OVERVIEW**

The contractor shall provide budget analysis support to the Budget Management Branch at NITC. Budget Analysis assignments may be internally focused within the branch or in support of an initiative coming from a customer or other organizational unit. Budget analysis services enable effective coordination and utilization of all other support services by planning and review of program execution with a goal of providing value to NITC customers for services received.

### **2. SCOPE/DUTIES**

- a) The contractor shall support budget analysis tasks that include monitoring budget reservations and executions, initiating execution of accounting transactions, analyzing and reconciling transactions with budget plans, and assuring compliance with regulations, directives, procedures, and guidelines.
- b) The contractor shall be fully responsible for the preparation and maintenance of business-line level spend plans and the complete tracking of funds reservations and execution by Standard General Ledger (SGL) account.
- c) The contractor shall support internally focused requirements/tasks and provide deliverables, which may include, but are not limited to, the following: reconciliation of accounts and income; assisting with analysis of reports, completion of documentation; preparation of document packages for audit review; and analysis of budget data. The contractor may be assigned to either a single or multiple NITC business lines, which may consist of between 400 and 600 budget line items.
- d) The contractor shall prepare, submit, and maintain BOC Rollup Summary reports identifying planned requirements, SGL account execution, and expected rest-of-year requirements broken down by Mandatory, Center Capacity, and Discretionary. Additional breakdowns showing current-month and rest-of-year amounts may be required. The BOC Rollup Summary shall also include a version-over-version explanation of changes to spend plan amounts by BOC Rollup. The BOC Rollup Summary reports shall be delivered at specified mid-month and end-of-month management briefing dates. The contractor shall assist in creating and executing a project plan and intermediate goals needed to meet these deliverable dates.
- e) The contractor shall prepare, submit, and maintain monthly Working Capital Fund (WCF) operating plan versus actual variance reporting results and explanations for current fiscal years using the required WCF tool & NITC format. The reporting results and related information shall be delivered no later than the Thursday immediately preceding the monthly WCF Status of Funds (SoF) reporting deadline (typically the 15<sup>th</sup> of each month).
- f) The contractor shall be responsible for the overall execution processing requirements (i.e. create, update, obtain signatures, etc.) and management of interagency agreements, purchase orders, reimbursable work authorizations, rental agreements, and other funds commitment documents.

- g) The contractor shall support externally focused requirements/tasks and provide deliverables, which may include, but is not limited to, providing other branches, offices, or agencies with budget data and analysis.
- h) Both types of support and deliverables (internally focused and externally focused) will require synthesis and presentation of data, development of alternative courses of action, and recommendations to decision makers. The contractor shall work with NITC senior management and internal NITC customers.
- i) Increased requirements associated with end-of-year financial activities will likely result in the need for the contractor to provide support that extends beyond a typical/standard work week (i.e. 40 hours) during the month of September. Requirements may increase by approximately 25% during this timeframe. The contractor shall fully support such requirements.

### **3. EXPERIENCE AND EXPERTISE REQUIREMENTS**

- a) Advanced Microsoft Office Excel skills.
- b) Working knowledge of General Accepting Accounting Principles (GAAP).
- c) Problem solving and analysis skills.
- d) Government accounting experience is preferred.



#### 4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Spend Plans and Tasks	<ul style="list-style-type: none"> <li>100% of spend plan documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.).</li> <li>100% of spend plan documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 2 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input
BOC Deliverables and Tasks	<ul style="list-style-type: none"> <li>100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents.</li> <li>100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 2 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input
WCF Deliverables and Tasks	<ul style="list-style-type: none"> <li>100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents.</li> <li>100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 2 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input

Usage Reconciliation Deliverables and Tasks	<ul style="list-style-type: none"> <li>▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents.</li> <li>▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 2 violations per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input
Inquiry Response	<ul style="list-style-type: none"> <li>▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 2 violations per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input
Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input

## **CLIN 003 - BUSINESS CONTINUITY PLANNING SERVICES**

### **1. OVERVIEW**

The Security Governance Branch, within the Security Division, is responsible for policies, controls and plans which ensure that risks are managed appropriately. The branch provides strategic direction, ensures that objectives are achieved, and verifies that the enterprises' resources are used responsibly and are consistent with applicable Federal laws and regulations. The Branch is made up of three teams: Contingency Planning, Risk Management, and Internal Audit.

The objective is to obtain services to support the NITC Business Continuity Program. The contractor shall develop IT disaster recovery (DR) and continuity of operations (COOP) plans and test schedules and shall coordinate and conduct COOP and DR tests.

The contractor may be required to make contact with NITC customers, technical staff, business partners, managers, and internal and external auditors.

### **2. SCOPE/DUTIES**

- a) The contractor shall work closely with the NITC Security Staff Contingency Management team and support the creation and maintenance of detailed DR plans for NITC IT systems, services and platforms in accordance with all applicable standards as identified by NITC, OCIO and applicable federal laws, regulations, policies and guidance.
- b) Conduct planning meetings with technical systems personnel to gather requirements and data required for the creation and documentation of IT DR plans for the Enterprise Data Center.
- c) Develop test schedules and plans, and support exercises for ITDR tests and call tree tests. Typically the NITC performs the following exercises:
  - i. Annually:
    - Four (4) notification (call tree) exercises.
    - Two (2) functional exercises.
    - Two (2) tabletop exercises.
  - ii. Monthly:
    - One (1) tabletop exercise.
    - Customer validation exercises, as required.
- d) Coordinate and track remedial actions, as necessary, following tests, training and exercises and create after action reports for presentation to NITC management by NITC staff.
- e) Perform business impact analysis for assigned IT systems, services or platforms. This includes the following:
  - i. Develop survey questions.
  - ii. Analyze documentation and/or survey results to ascertain which system, service or platform supports a mission critical business process.

- iii. Develop and present achievable recovery time objectives (RTO) and recovery point objectives (RPO) as it relates to internal or customer IT systems, services or platforms.
  - iv. Develop and propose DR strategies and plans stemming from analysis of documentation, surveys and discussions with subject matter experts (SME).
- f) Participate in special initiatives or projects where contingency planning or DR expertise is required. For example, assist in the planning and implementation of new DR strategies or processes. Assist in the publication and distribution of contingency planning documents.
- g) Develop and maintain COOP and DR documentation as it pertains to the accreditation of IT systems, services or platforms.
- h) Develop, maintain and deliver presentations regarding COOP and DR practices which include classroom training, workshops and formal or informal briefings to technical and senior NITC staff. Presentations and documents shall be developed using standard office automation tools such as Microsoft Office, Project and Visio.
- i) Provide routine technical knowledge transfer to identified NITC technical staff.
- j) Actively participate in meetings or discussions to provide status and resolve issues related to assigned IT systems, services or platforms.
- k) Perform analysis of security tasks to identify areas where there may be overlapping or redundant tasks which can be optimized or modified to create efficiencies or economies of scale on assigned IT systems, services or platforms.
- l) Respond to customer inquiries via email or telephone, from both internal and external customers, with timely, accurate information, within 24 hours.
- m) Maintain DR data in the LDRPS database.
- n) Maintain Call Tree data in the MIR3 system.

### **3. EXPERIENCE AND EXPERTISE REQUIREMENTS**

- a) Well versed in the technical areas of disaster recovery planning and business resumption planning for information technology operations.
- b) Expert level experience in developing and maintaining IT Disaster Recovery (ITDR) Plans, coordinating ITDR exercises, developing ITDR test and exercise plans, auditing tests and exercises in order to determine weaknesses, strengths, and remedial actions required to ensure effective recovery capabilities for a large Federal data center, and preparing after action assessments, reports and lessons learned.
- c) Experience in developing and conducting business impact assessments (BIA), analyzing results of BIAs and coordinating with technical teams to develop recovery solutions based on BIA results.
- d) Experience conducting and assessing emergency alert and notification drills, documenting test, training and exercise plans and after action reports.
- e) Experience developing or maintaining Business Continuity Plans, Continuity of Operations Plans, and Crisis Communications Plans. This includes interviewing subject matter personnel to ascertain the mandatory elements of various types of contingency plans.

- f) Experience in preparing and giving disaster recovery and emergency response presentations for customers.
- g) Sound knowledge of Federal directives regarding continuity of government and continuity of operations requirements or a sound knowledge of national standards for disaster or emergency management and business continuity programs for private industry.
- h) Experience providing advice and assistance in the following: developing overall continuity of operations strategies, emergency response, team deployment, employee and family assistance for trauma, human capital planning for emergencies, emergency operations, guidelines for determining and operating at alternate facilities, and incident management.
- i) Proficient using MS-Word, MS-Excel and MS-Project software, and possess strong abilities in writing technical documents. The contractor must have experience in facilitating meetings.

#### 4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
DR and COOP Plans and Tasks.	<ul style="list-style-type: none"><li>▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant with applicable governing regulations, policies, directives and guidance.</li><li>▪ 100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li></ul>	<ul style="list-style-type: none"><li>▪ No more than 2 violations per month.</li><li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li></ul>	<ul style="list-style-type: none"><li>▪ CPARS assessment ratings.</li><li>▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00.</li></ul>	Checklist and Customer Input

DR and COOP Test Documentation and Tasks.	<ul style="list-style-type: none"> <li>▪ 100% of documentation is prepared via the utilization of required tools as applicable.</li> <li>▪ 100% of test schedules, methods, and activities shall be coordinated with all required participants and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> <li>▪ 100% of participants shall have access as required to successfully participate in test activities.</li> <li>▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant with applicable governing regulations, policies, directives and guidance.</li> <li>▪ 100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 2 violations per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Weekly Status Report	<ul style="list-style-type: none"> <li>▪ 100% complete.</li> <li>▪ 100% accurate.</li> <li>▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 1 violation per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input

Inquiry Response	<ul style="list-style-type: none"> <li>Respond to all customer inquiries NLT 24 hours after inquiry receipt.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 2 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input



## **CLIN 004 - ENTERPRISE INFORMATION TECHNOLOGY SERVICES PORTFOLIO MANAGEMENT**

### **1. OVERVIEW**

The Service Portfolio Branch manages the portfolio suite of technology services, and accompanying business processes that enable the United States Department of Agriculture (USDA) to achieve its goals and objectives of eGovernment, leveraging its investments and delivering government services in a more citizen-centric manner.

The services offered by the National Information Technology Center (NITC) Enterprise Data Center (EDC) are enterprise-wide. Department, Agency, or Federal eGovernment initiatives can leverage these services. USDA Agencies and initiatives do not have to create their own technology solutions and standards and can instead utilize the NITC EDC centralized service offerings to support their business requirements and thus avoid the high cost and high learning curve of operating these solutions independently.

### **2. SCOPE/DUTIES**

- a) Services Architecture. The contractor shall support tasks including, but not limited to, the following:
  - i. Participate in identifying and prioritizing the next steps for the technical environments. As agency use increases, components of the architecture are upgraded, and new requirements surface, changes to the service offering may be necessary to assure that the technical environments, the application support as well as the financial impact are fair, equitable and functioning as expected. Any deviations from these service scopes will need to be identified as early as possible, planned and tracked to implementation.
  - ii. Identify and managing new services offerings from cradle to grave.
  - iii. Plan support of and integration with any new service offerings, such as collaboration or records management. This includes discussions with NITC technical teams to determine the necessary steps to support new offerings such as identifying hardware and software components as well as identifying customized code that might be necessary to support the service in the existing architecture.
  - iv. Develop technical standards for all environments. These standards should follow best practices and support the NITC EDC architecture.
- b) Agency Liaison / Software Consulting. The contractor shall support tasks including, but not limited to, the following:
  - i. Facilitate agency meetings and workshops. As agencies express interest in the use of the NITC EDC service offerings and want to develop applications in this framework, a pre-implementation meeting will occur between agency teams and the NITC Account Manager, with support from the Agency Liaison. Workshops may be scheduled to expedite agency planning and implementation of requirements. This support involves meeting logistics, preparation of materials, and planning work prior to and after the meeting to correctly guide the agency through the processes of transitioning to NITC EDC services. Additionally, the Agency Liaison

shall provide support with technical details and information about the architectures of NITC EDC services.

- ii. Agency Adoption Support. Agency Liaisons and their government NITC EDC Business Development counterpart will work directly with agencies to support their use of NITC EDC services. This support will include initial discussion of the tools and their abilities, coordination of tool access, and communication with data center and operations entities. In the longer term, this support will include a marketing aspect as well as communicate to the agencies the proper use of the tools and the services.

### **3. EXPERIENCE AND EXPERTISE REQUIREMENTS**

- a) Experience with overall enterprise data center services life cycle development as well as the development and maintenance of service catalogs, in support of the organizational mission.

#### 4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Product Management Analysis Deliverables and Tasks	<ul style="list-style-type: none"><li>▪ 100% of applicable service offerings shall be analyzed and reported within the applicable annual period.</li><li>▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.), to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.</li></ul>	<ul style="list-style-type: none"><li>▪ No more than 4 violations per month.</li><li>▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li></ul>	<ul style="list-style-type: none"><li>▪ CPARS assessment ratings.</li><li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li></ul>	Checklist and Customer Input

Portfolio Services Deployment Deliverables and Tasks	<ul style="list-style-type: none"> <li>▪ 100% of on-going documentation and reporting of NITC Service Development milestone achievements shall be provided for new services proposed from the NITC Service Development Portal as defined by the NITC Service Development Lifecycle Directive.</li> <li>▪ 100% attendance and active participation in all facilitation/collaboration/consultation events as required.</li> <li>▪ 100% of facilitation/collaboration/consultation presentations and communications shall be coordinated as required and shall be clear, effective, concise, and organized.</li> <li>▪ 100% of facilitation/collaboration/consultation activities shall be tailored specifically for subject matter needs and shall result in the team's ability and empowerment to achieve documented action items and milestones.</li> <li>▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 4 violations per month.</li> <li>▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> <li>▪ Facilitation ineffectiveness may be determined to be a violation.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
--	--	---	---	---------------------------------------

Documentation	<ul style="list-style-type: none"> <li>▪ 100% of all NITC Service Catalog documentation shall be produced and maintained, including the performance and documentation of required modifications/adds/deletes, to ensure accurate representation of NITC Service offerings.</li> <li>▪ 100% of all NITC Services Appendices documentation shall be produced, edited, reviewed, distributed and maintained, including the performance and documentation of required modifications/adds/deletes, to ensure accurate representation of NITC Service offerings.</li> <li>▪ 100% of documentation shall be updated IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.</li> <li>▪ Electronic versions of all documentation in the required format shall be posted/stored in the required artifact repository/tool location within the mutually established timeframe and shall be available for Government review at all times as required.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 4 violations per month.</li> <li>▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Weekly Status Report	<ul style="list-style-type: none"> <li>▪ 100% complete.</li> <li>▪ 100% accurate.</li> <li>▪ Submitted no later than (NLT) 2<sup>nd</sup> business day of the calendar week following the reporting period.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 1 violation per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input

Inquiry Response	<ul style="list-style-type: none"> <li>Respond to all customer inquiries NLT 24 hours after inquiry receipt.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 4 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input

## CLIN 005 - FACILITIES OPERATIONS SERVICES

### 1. OVERVIEW

The objective of this CLIN is to obtain technical support services for the National Information Technology Center (NITC) Data Center in support of ~~the Service Portfolio Branch~~ **datacenter facilities**. The contractor shall serve as a Facilities Operations Specialist responsible for project management activities in support of data center mission capabilities, including change, problem and inventory management. The contractor shall support the overall operation of the data center and oversees data center facilities plans and proposals as well as ensuring all security requirements are met in accordance with Government guidelines and standards. The contractor shall assist in and support increasing program effectiveness by evaluating current facility operation services and assisting in the development of new services. This position may require making contacts with NITC customers, technical staff, business partners, management, and internal/external auditors.

### 2. SCOPE/DUTIES

- a) Plans and develops electrical power needs for new and existing equipment in the Centers by applying a thorough and practical knowledge of engineering methods and techniques. Takes into account characteristics of electrical power systems to draft, design, analyze and review plans for power distribution, ground grid systems, electrical circuitry, size of conduit, wire, etc., necessary for installing Center support systems. Translates plans into specification tasks as required. The contractor shall assist the NITC facilities manager as required, to include the updating of existing documentation or creation of new documentation using Microsoft Office products, and AutoCAD.
- b) Monitoring of office and computer room environmental conditions such as air conditioning, heat, power, generators, and air plenum to ensure computer system availability as required. Identifies and analyzes potential problems and prepares alternative solution for consideration. The contractor shall follow procedures and instructions to specify method of repair, modification, maintenance and testing of environmental systems.
- c) Identifies electrical, space, and cooling requirements for new IT hardware. Monitors environmental controls to ensure the computer room is operating at peak performance at all times. Physically assists when needed to support the installation of hardware in rack space on the data center floor; setting up conference rooms; assisting with day to day facility operations; documenting equipment installation, configuration, and electrical connection; and distribution of applicable documentation to asset management personnel as required.
- d) Perform quality assurance activities in support of maintenance operations.
- e) Submit recommendations and justifications to modernize or improve structures and equipment. Provides input into performance profile surveys, equipment inspections, technical troubleshooting, maintenance evaluations, and workload analysis.
- f) Review, analyze and evaluate deficiency reports and equipment malfunction reports. Considers significance of failures in regard to safety hazards, cost of repairs, loss or downtime of equipment, and delays resulting from lack of available parts.

- g) Evaluate and determine the quality and quantity of repair parts and tools to reduce unnecessary duplication and variety, as well as to ensure that needed materials are on hand.
- h) Perform preparation and restoral activities associated with the installation and removal of equipment related to work areas consisting of heating, ventilating, air conditioning, high/low voltage electrical, carpentry, painting, masonry, sheet metal work and similar trades. Prepare inspection reports for the purpose of identifying and recommending solutions to problems involving lack of personnel, materials, poor workmanship, conditions in need of repair, and various other related concerns.
- i) Responsible for facilities related hardware systems ingress and egress from the data center floor. Receives and installs hardware from agencies or vendors. Determine power requirements and coordinate electrical service installation for hardware. Support the procurement and complete the installation of low voltage cabling to provide connectivity to existing systems and to internal KVM monitoring systems.

### **3. EXPERIENCE AND EXPERTISE REQUIREMENTS**

- a) Overall project management of secure data center facilities projects, including projects related to the infrastructure systems and equipment of the center.
- b) Experience with the management of mechanical, electrical, and environmental requirements associated with a computer room environment.
- c) Working knowledge of computer protection devices and environmental systems, including, but not limited to, the following: uninterruptible power systems, diesel generators, transfer switches, paralleling gear, computer room air-conditioning, security, and fire protection systems.



## 1. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Facility Technology Analysis Deliverables and Tasks	<ul style="list-style-type: none"> <li>100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.), to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 2 violations per month.</li> <li>Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input
Design and Implementation Planning Deliverables and Tasks	<ul style="list-style-type: none"> <li>100% of documentation shall be clear, concise, organized and developed with required tools as applicable.</li> <li>100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 2 violations per month.</li> <li>Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input

Documentation Updates and Storage/Repository	<ul style="list-style-type: none"> <li>▪ 100% of documentation shall be updated IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.</li> <li>▪ Electronic versions of all documentation in the required format shall be posted/stored within the mutually established timeframe in the required artifact repository/tool location and shall be available for Government review at all times as required.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 2 violations per month.</li> <li>▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input
Weekly Status Report	<ul style="list-style-type: none"> <li>▪ 100% complete.</li> <li>▪ 100% accurate.</li> <li>▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 1 violation per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input
Inquiry Response	<ul style="list-style-type: none"> <li>▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 2 violations per month.</li> <li>▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$1,500.00.</li> </ul>	Checklist and Customer Input

Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input
---	--	--	--	------------------------------

## CLIN 006 - INFORMATION SYSTEMS SECURITY SUPPORT SERVICES

### 1. OVERVIEW

The Security Governance Branch, within the Security Division, is responsible for policies, controls and plans which ensure that risks are managed appropriately. The branch provides strategic direction, ensures that objectives are achieved, and verifies that the enterprises' resources are used responsibly and are consistent with applicable Federal laws and regulations. The Branch is made up of three teams: Contingency Planning, Risk Management, and Internal Audit.

The objective is to obtain technical support for the Risk Management Team's (RMT) mission of performing the continuous authorization tasks of the USDA's Continuous Assessment and Authorization (A&A) process of the current version of the USDA Six Step Risk Management Framework (RMF) Process ([USDA Six Step Risk Management Framework Process \(RMF\) Guide](#)). The contractor may be required to make contact with NITC customers, technical staff, business partners, managers, and internal and external auditors.

### 2. SCOPE/DUTIES

a) The scope covers the systems listed in the NITC Systems table below.

System Name	Acronym	System Type	Assessment Type
NITC Enterprise Services	ES	General Support System	Cont. Assess. A-123
NITC Auxiliary Support System	AXS	General Support System	Cont. Assess. A-123
NITC Customer Billing System	CIMS	Major Application	Cont. Assess. A-123
NITC Data Center	NITC Data Center	Site	Cont. Assess. A-123
NITC Internal Services	NIS	Site	Cont. Assess. A-123
NITC ITSM Services Environment	ISE	Major Application	Cont. Assess.
NITC Mainframe	NITC Mainframe	General Support System	Cont. Assess. A-123
NITC Management Support System	MSS	Minor Application	Cont. Assess.
NITC Midrange Systems	NITC Midrange	General Support System	Cont. Assess. A-123
NITC Telecommunications Network GSS	NITC Network	General Support System	Cont. Assess. A-123
NITC Infrastructure GSS	NITC IaaS	General Support System	Cont. Assess

- b) For the systems listed as "Cont. Assess." (Continuous Assessment), the contractor shall perform the continuous authorization tasks of continuous assessment and authorization (A&A) process following Step 6 of the RMF process and makes applicable updates to all control documentation within the boundary of the system in scope.
- c) The contractor shall review and update the system security plan, , annually according to the timeframes assigned within the Level Workload Schedule (LWS).
- Review and update the system security plan.
    - General Description
    - The Mission/Purpose
    - The Information Types (the Statement of Security Needs (SOSN))

- The Locations
- The Interconnections
- The System Description and Technical Description Narratives
- The Points of Contact.
- All security controls applicable to the system.
- The appendices:
  - K2 - MOU/SLA Agreements
  - L - Contingency/Disaster Recovery Plans
  - O - Incident Response Plan (facilitate updates)
  - Q2 - Configuration Management Plan (facilitate updates)
  - R - Accreditation Statement and Documentation
  - S - Hardware Listing
  - T - Software Listing
  - V2 - Privacy Threshold Analysis
  - V3 - Privacy Impact Assessment
- ii. Working with control owners, review and update the appropriate control Implementation Statements for all controls that apply to each system
- iii. Upon completion of the above tasks (identified as i and ii), manage the process of completing the Step 6 documentation Concurrency Review and work with the control owners to make updates needed based on concurrency review findings.
- d) The contractor shall update control sets when revisions to National Institute of Standards and Technology Special Publication (NIST SP) 800-53, and other applicable regulations and guidance, are adopted by the agency.
- e) Develop and execute a project plan(s) that defines responsibilities, timelines, deliverables, risks, and milestones necessary to accomplish the objectives of the task.
- f) Provide a weekly project status report, orally and in writing.

### **3. EXPERIENCE REQUIRED**

- a) Working knowledge of the technical requirements of applying the Risk Management Framework to Federal information systems in an enterprise Federal data center.
- b) Working knowledge of the technical requirements of applying the Federal Risk and Authorization Management Program (FedRAMP) requirements to Federal information systems in a large Federal data center.
- c) Proficient using MS-Word, MS-Excel and MS-Project software, and possess strong abilities in writing technical documents. Skilled in facilitating meetings.

#### 4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Security Plans and Tasks	<ul style="list-style-type: none"> <li>100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant all with applicable governing regulations, policies, directives and guidance.</li> <li>100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 6 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> <li>No more than 10 findings resulting from the first round of the Step 3 Concurrency Review, and those findings are corrected within 5 business days.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Implementation Statements and Tasks	<ul style="list-style-type: none"> <li>100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant all with applicable governing regulations, policies, directives and guidance.</li> <li>100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 6 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input

Project Planning and Management (including Step 3 Concurrency Review)	<ul style="list-style-type: none"> <li>▪ The contractor shall develop, document, and maintain project plans 100% compliant with federal governing regulations, policies, directives, guidance and industry practice.</li> <li>▪ 100% of project plans shall include the identification of applicable responsibilities, timelines, deliverables, risks, milestones and other elements as required.</li> <li>▪ 100% of plan schedules and activities shall be coordinated with all required participants.</li> <li>▪ All issues impacting project schedules shall be communicated to government staff within one business day after determination of impact.</li> <li>▪ 100% of project plans shall be updated weekly.</li> <li>▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.).</li> <li>▪ 100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 6 violations per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Weekly Status Report	<ul style="list-style-type: none"> <li>▪ 100% complete.</li> <li>▪ 100% accurate.</li> <li>▪ Submitted no later than (NLT) 2<sup>nd</sup> business day of the calendar week following the reporting period.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 1 violation per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input

Inquiry Response	<ul style="list-style-type: none"> <li>Respond to all customer inquiries NLT 24 hours after inquiry receipt.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 6 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input



## **CLIN 007 - INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM) PROCESS DEVELOPMENT AND DOCUMENTATION SERVICES**

### **1. OVERVIEW**

The objective is to obtain Information Technology Service Management (ITSM) process development and documentation support for the National Information Technology Center (NITC), Infrastructure Operations Division, IT Service Management Branch (IOD/ITSMB). This position may require making contacts with NITC customers, technical staff, business partners, management, and internal/external auditors.

### **2. SCOPE/DUTIES**

- a) Perform process gap analysis, monitor and assess defined key performance indicator (KPI) and metrics.
- b) Develop and manage the software development lifecycle artifacts including Business, Functional and Technical Requirements, Functional Design Documents, Use Cases, Process Models, Data Flow Diagrams, etc., as required.
- c) Develop software and technology requirement specification documents, as required. Liaise with the Service Transition Process Owners, Process Managers, NITC IT and Business Staff throughout Process Analysis, Design, Development, Testing and Implementation for Service Transition process improvements.
- d) Create, facilitate and develop end user acceptance testing plans according to the documented business, functional and technical requirements and process design documents necessary to meet business process and technology requirements.
- e) Provide end user process training materials, as required.
- f) Plan and coordinate new service design packages through the Service Transition model, as required.
- g) Create, test and release, change request templates and task templates for Service Request Fulfillment and Change Management process and technology requirements.
- h) Create IT Service Transition procedures and processes as required.

### **3. EXPERIENCE AND EXPERTISE REQUIREMENTS**

- a) Expert-level analytical and problem-solving skills.
- b) Certified in ITIL Foundations v3.
- c) Ability to manage multiple requirements simultaneously
- d) Experience with ITSM technical writing.
- e) Proficiency in MS Office products.
- f) BMC Remedy Enterprise Suite experience.

#### 4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
ITSM Process Development and Documentation Services Task/Product Activities	<ul style="list-style-type: none"> <li>100% of all ITSM Process and Development and Documentation activities shall be conducted in accordance with governmental &amp; organizational standards, policies, directives, standard operating procedures, work instructions, processes &amp; guidance. All operational support activities shall be captured and properly documented in the organizational ITSM tool. The contractor shall adhere to this requirement unless a written exemption is issued by an authorized Government representative.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 2 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$10,000.00.</li> </ul>	Checklist and Customer Input
Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input

# **CLIN 008 - INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM) SERVICE ASSET AND CONFIGURATION MANAGEMENT SUPPORT SERVICES**

## **1. OVERVIEW**

The contractor shall provide Service Asset and Configuration Management support across the various organizational units at the National Information Technology Center (NITC). Service Asset and Configuration Management coordination, within the current environment, may require the contractor to provide direct support to NITC customers, technical staff, management, and internal and external auditors.

The contractor shall perform in a Service Asset and Configuration Management specialist capacity supporting the maintenance, administration, quality and accuracy of the NITC Service Asset and Configuration Management centralized data repository, Configuration Management Database (CMDB) through the asset management applications.

## **2. SCOPE/DUTIES**

The Government will issue contractor task assignments via the organization ITSM suite.

- a) The contractor shall support internally focused requirements/tasks and provide deliverables, which may include, but are not limited to, the following: managing Atrium CMDB Configuration Item (CI) updates along with other associated asset information, data analysis, auditing and reporting, measure performance and data quality, and administration of the Atrium Core console functions such as automated or manual data normalization and reconciliation.
  - i. Atrium CMDB Updates
    - Perform assigned end user requested CI quality updates via incident service request tickets and approved change records.
    - Perform automatically assigned CI update tasks from within submitted and approved change records.
    - Perform assigned product catalog and Definitive Media Library (DML) item updates via submitted and approved change records.
    - Perform assigned end user requested inventory location updates via incident service request tickets and approved change records.
    - Perform end user requested customer project updates including the changing of CIs related to projects via submitted and assigned incident service request tickets and approved change records.
    - Perform end user requested master contract updates including the changing of CIs related to contracts via submitted and assigned incident service request tickets and approved change records.
    - Perform technical or business service CI updates for Atrium Discovery and Dependency Mapping (ADDMM) application to service discovered CIs via submitted and approved change records.
  - ii. Atrium CMDB Reporting

- Perform scheduled queries, exports and reports of CI or other CMDB related data by the defined format and store within designated file locations. Scheduled queries, exports and reports include, but are not limited to:
    - Full Hardware CI Export
    - Full Dataset Export (all datasets configured)
    - CIs Created in past 30 days
    - CIs Decommissioned in past 30 days
    - CIs disposed in past 30 days
    - CIs received in past 30 days
    - Percentage and count of CIs discovered by ADDM (scanning and discovery tool)
    - Percentage and count of CIs not discovered by ADDM (scanning and discovery tool)
    - Percentage and count of CIs with incomplete, required attributes
    - Percentage and count of Unauthorized CIs (created or updated without a change record)
    - Percentage and count of CIs unidentified or identified incorrectly by platform service, service role, service rate, project and customer agreement
  - Perform assigned end user requested ad-hoc CI exports or reports via incident service request tickets.
  - Update Standard Operating Procedures (SOPs) that are affected by government changed Service Asset and Configuration Management policies, process or CI or other related data specifications.
- iii. Atrium CMDB Administration
- Run and monitor manual atrium reconciliation and normalization jobs and resolve errors according to defined procedures.
  - Perform manual atrium identification on all reconciliation jobs and resolve conflicts or errors according to defined procedures.
  - Identify and verify IT infrastructure configuration items such network, security, hardware and software assets and the relationships between them.
- b) The contractor shall support externally focused requirements/tasks and provide deliverables which may include, but are not limited to, providing other branches, offices, or agencies with asset data and analysis. Both types of deliverables will require presentation of data, development of alternative courses of action, and recommendations to decision makers.
- c) The contractor shall implement and employ Service Asset and Configuration Management IT Infrastructure Library (ITIL) processes and principles that are aligned with NITC approved policy.
- d) The contractor shall provide weekly status reporting to the Alternate Contracting Officer's Representative – Technical (ACORT).

### **3. EXPERIENCE AND EXPERTISE REQUIREMENTS**

- a) BMC Atrium CMDB.
- b) BMC ITSM suite.

- c) Well developed personal computing skills and knowledge of standard MS Office Products, such as Outlook, Excel and Word. The ability to generate accurate ADHOC reports using these programs is required.
- d) Teamwork, coordination, analytical thinking, problem-solving, and documentation are critical aspects of success in performing the required tasks.

#### 4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
ITSM Service Asset and Configuration Management Task/Product Activities	<ul style="list-style-type: none"> <li>100% of all ITSM Service Asset and Configuration Management activities shall be conducted in accordance with governmental &amp; organizational standards, policies, directives, standard operating procedures, work instructions, processes &amp; guidance. All operational support activities shall be captured and properly documented in the organizational ITSM tool. The contractor shall adhere to this requirement unless a written exemption is issued by an authorized Government representative.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 2 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$10,000.00.</li> </ul>	Checklist and Customer Input
Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input

## **CLIN 009 - PROGRAM/PROJECT MANAGEMENT SUPPORT SERVICES**

### **1. OVERVIEW**

The contractor shall provide project management support across the various organizational units at the National Information Technology Center (NITC). Project management assignments may be internally focused or in direct support of a customer initiative. Internally focused projects may include infrastructure upgrades, software version upgrades, security implementations, and development of new service offerings. Externally focused projects may include customer business application migrations from one data center hosting platform to another, customer disaster recovery support, and customer business application migration to the data center from an external hosting provider. The Government will issue written project assignments to the contractor. The contractor shall implement and employ project management methodologies that are aligned with NITC approved policy.

Project Management coordination, within the current environment, may require contractor staff to provide direct support to NITC customers, technical staff, business partners, management, and internal and external auditors.

### **2. SCOPE/DUTIES**

- a) General Tasks. General tasks include, but are not limited to, the following: managing internal and external projects utilizing the tools and methodology defined by the NITC Project Management Office (PMO); refining, enhancing, and improving the NITC PMO toolset, methodology, and practices; knowledge transfer and informal training; reporting status to Alternate Contracting Officer's Representative – Technical (ACORT); management of a project's critical path; and facilitating organization change towards a more project management oriented culture. Teamwork, coordination, and documentation are critical aspects of success in performing the tasks.
- b) Initiating Phase. The contractor shall perform processes to define a new project or new phase of an existing project by completing work to establish the project charter and gain Government/stakeholder acceptance. Depending on projected cost of the project, the initiation phase may be governed by the Office of the Chief Information Officer's (OCIO's) Capital Planning and Investment Control thresholds. Tasks include, but are not limited to, the following: documenting objectives, developing a project charter, identifying a project sponsor and stakeholders, defining high level deliverables, projecting deliverable completion dates, identifying resource requirements, and gaining Government approval. Required templates include: Project Charter, Project Weekly Status Report and/or Minor Project Weekly Status Report.
- c) Planning Phase. The contractor shall perform processes to identify the tasks and work assignments to complete an approved project charter. Tasks include, but are not limited to, the following: estimating schedules, sequencing tasks, documenting risks, developing risk mitigation strategies, documenting project alternatives/assumptions/constraints. Required templates include: Work Breakdown Structure, Risk Matrix, and Project Weekly Status Report.

- d) Executing Phase. The contractor shall perform activities such as project team facilitation, project team solution generation, project team coaching for breakthrough performance, project management plan monitoring, project deliverable tracking, and management reporting. The contractor shall possess “people skills” to gain the confidence, trust and respect throughout the organization while ensuring that project team members are treated with dignity and respect. Through the project monitoring activities, the contractor shall ensure that the work breakdown structure correctly identifies the critical path tasks/work activities within one (1) business day of identifying a deviation. Required templates include: Work Breakdown Structure, Critical Path Diagram, and Project Weekly Status Report.
- e) Controlling Phase. The contractor shall perform analysis activities to compare actual performance with planned performance, identify and report variances, evaluate possible migration strategies, perform earned value management (when required), recommend appropriate corrective actions, and communicate to seek guidance from the Project Sponsor (Stakeholders), as applicable.
- f) Close Out Phase. The contractor shall perform activities to assemble project artifacts in a historical repository. Tasks include, but are not limited to, the following: formalizing customer acceptance, preparing a final project performance report, documenting lessons learned, and archiving project records.
- g) The contractor shall support all meeting and reporting requirements.

### **3. EXPERIENCE AND EXPERTISE REQUIREMENTS**

- a) Project Management Professional (PMP) certification.
- b) Experience with Government EVM requirements is preferred.



#### 4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Project Planning and Management Deliverables and Tasks	<ul style="list-style-type: none"> <li>100% adherence to mutually agreed upon project management tasks, activities, and objects/artifacts established and documented in the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.).</li> <li>The contractor shall develop, document, and maintain project plans 100% compliant with federal governing regulations, directives, guidance and industry practice.</li> <li>100% of project plans shall include work breakdown structures, critical paths, estimated resources, risk matrices and other elements as required.</li> <li>100% of plan schedules and activities shall be coordinated with all required participants.</li> <li>The contractor shall communicate all issues impacting project schedules to government staff within one business day after determination of impact.</li> <li>Changes to project plans shall be updated within mutually established time parameters.</li> <li>100% of documentation and services (including updates) shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> <li>100% of documentation and services (including updates) shall be completed and submitted IAW the requirements established within the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 6 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input

Project Management Team Facilitation	<ul style="list-style-type: none"> <li>▪ 100% of facilitation presentations and communications shall be coordinated as required and shall be clear, effective, concise, and organized.</li> <li>▪ 100% of facilitation activities shall be tailored specifically for team needs and shall result in the team's ability and empowerment to achieve documented action items and milestones.</li> <li>▪ Facilitators shall respond to 100% of questions and requests with applicable responses/references.</li> <li>▪ 100% of documentation and services (including updates) shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> <li>▪ 100% of documentation and services (including updates) shall be completed and submitted IAW the requirements established within the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 6 violations per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Weekly Status Report	<ul style="list-style-type: none"> <li>▪ 100% complete.</li> <li>▪ 100% accurate.</li> <li>▪ Submitted no later than (NLT) 2<sup>nd</sup> business day of the calendar week following the reporting period.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 1 violation per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input

Documentation Repository	<ul style="list-style-type: none"> <li>Current electronic versions of all documentation in the required format shall be posted within the mutually established time parameters in the artifact repository and shall be available for Government review at all times as required.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 6 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Inquiry Response	<ul style="list-style-type: none"> <li>Respond to all customer inquiries NLT 24 hours after inquiry receipt.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 6 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input

## **CLIN 010 - TASK ORDER MANAGEMENT**

### **1. OVERVIEW**

The contractor shall provide complete task order management as required to ensure successful completion of all task order requirements in accordance with the terms and conditions of the task order.

### **2. SCOPE/DUTIES**

The minimum requirements associated with task order management are identified below.

- a) The task order management team shall include one Task Order Manager (TOM) whom is responsible for the overall task order performance and whom shall act as the primary liaison between the individual contractor employees and the Government. The name of the primary TOM and alternate(s) TOM, who shall serve as the TOM when the primary TOM is absent, shall be designated in writing to the Contracting Officer (CO) at the time of award.
- b) The contractor shall clearly define the duties to be performed by all contractor personnel to ensure a clear distinction between task order management support and operational support that is performed under one or more other Contract Line Item Numbers (CLINs) as described in PWS paragraph 5.1 (i.e. non-task order management). A full explanation with sufficient information demonstrating how the operational duties will not be affected by the task order management duties will be required for all contractor personnel proposed to provide support in multiple areas (i.e support the task order management CLIN and any other CLIN(s)).
- c) The Contractor personnel are under the administrative control of the Contractor. The Contractor shall be solely responsible for the complete supervision and management of its personnel under the task order. The Contractor shall select, supervise, and exercise control and direction over its personnel under this task order. The Government shall not supervise, direct, or control the activities of Contractor personnel. The Contractor shall not exercise any supervision or control over the Government in performance of contractual services.
- d) The Contractor's TOM shall meet monthly (or more frequently if needed) with the COR or Government project staff to communicate work status; discuss accomplishments or problems; and propose solutions and enhancements of services. The TOM shall identify methodologies and performance schedules to ensure work is progressing satisfactorily. The COR will establish and relay priorities for tasks and projects at these meetings and communicate directly with the TOM. Acceptance criteria, areas of outstanding performance, and any failure to meet task order requirements, along with necessary corrective action, will be discussed and shall be documented.
- e) The contractor shall schedule, facilitate, and document a Program Management Review (PMR) each quarter with NITC and GSA representatives for the duration of the task order, unless otherwise directed. The PMR shall be a forum to review and discuss the following: overall task performance including significant accomplishments; issues and

risks; additional areas of needed support; potential resource allocation adjustments; and other items deemed essential at a later date.

- f) The contractor shall provide general task order management support to include, but not be limited to, the tasks identified below.
  - i. The contractor shall provide a task order management plan that describes the technical approach, organizational resources, and management controls proposed for task performance.
  - ii. Manage all overall task performance.
  - iii. Assign and manage contractor work schedules to ensure the necessary coverage is provided in accordance with the task requirements.
  - iv. Review work discrepancies.
  - v. Disseminate communicating policies, purposes and goals of the client organization(s) to contractor personnel providing task order support as applicable.
  - vi. Track expiration of system access (LincPass) badges to ensure re-enrollment is accomplished a minimum of 30 days prior to expiration.
  - vii. Management, to include scheduling and monitoring, of overall contractor personnel training to ensure compliance with the training requirements identified in PWS paragraph 6.3. Provide the COR and/or the applicable Government representative with a minimum of 30 days advance notice of when employees will be absent for training purposes.
  - viii. Complete travel requests (shall use required template) in accordance with the travel requirements identified within PWS paragraph 9.4.2 and ensure sufficient travel funds are available to support such requests.
  - ix. Attend meetings beyond those identified in paragraph (d) above.
  - x. Notify the ACORT (by telephone or email) when an employee will be absent, within 1 hour of awareness of an unscheduled absence, to minimize any negative impact to daily task activities.
  - xi. Maintain up-to-date lists of Government Furnished Equipment (GFE) and Government Furnished Items (GFI). Such lists shall be made available to the Government upon request.
  - xii. Development and submission of a monthly status report.
  - xiii. Meet with the respective ACORT's on a regular basis, estimated to be bi-monthly, to discuss workloads, progress on projects, and performance issues/problems.
  - xiv. Provide a monthly calendar of contractor personnel scheduled absences for the next two months as an appendix to the monthly status report.

### **3. EXPERIENCE AND EXPERTISE REQUIREMENTS**

- a) Expertise in human resource management, supervision, leadership, conflict resolution, interpersonal skills, and internal controls.
- b) Management experience, including expertise in the management and control of funds and resources using complex reporting mechanisms and demonstrated ability in managing multi-task awards and/or subcontract awards of various types and complexity.
- c) Experience and expertise in the Information Technology (IT) industry.

#### 4. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Monthly Status Report	<ul style="list-style-type: none"> <li>100% complete with all required appendices.</li> <li>100% accurate.</li> <li>Submitted no later than (NLT) 15th calendar day of month following the reporting period and submitted concurrent with the monthly invoice.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 5 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00</li> </ul>	Checklist and Customer Input
Monthly Invoice	<ul style="list-style-type: none"> <li>100% complete with all required supplemental information.</li> <li>100% accurate.</li> <li>Submitted no later than (NLT) 15th calendar day of month following the reporting period and submitted concurrent with the monthly status report.</li> </ul>	<ul style="list-style-type: none"> <li>No violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each violation will result in a payment reduction of 5% up to the maximum reduction of \$10,000.00.</li> </ul>	Checklist and Customer Input
Scheduled Absence Calendar Availability	<ul style="list-style-type: none"> <li>A current electronic version shall be available for Government review at all times.</li> <li>The calendar shall be 100% accurate.</li> </ul>	<ul style="list-style-type: none"> <li>No violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or unavailability.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each violation will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input

LincPass Status	<ul style="list-style-type: none"> <li>▪ No expirations of valid LincPass accounts.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> <li>▪ Each violation will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Other Task Specific Requirements and Deliverables	<ul style="list-style-type: none"> <li>▪ 100% adherence to mutually agreed upon management tasks, activities, and objects established and documented in the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.).</li> <li>▪ 100% of documentation and services shall be completed and submitted NLT the established date for completion/receipt as identified in the requirement documents.</li> <li>▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No more than 1 violation per month.</li> <li>▪ A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> </ul>	Checklist and Customer Input

Mandatory Government Training Compliance	<ul style="list-style-type: none"> <li>100% of the training (for all contractor personnel performing under the task order, including all CLINs) shall be completed and submitted NLT the established date for training completion as mandated by the Government.</li> </ul>	<ul style="list-style-type: none"> <li>No violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each violation will result in a payment reduction of \$1,000 up to the maximum reduction of \$15,000.00.</li> </ul>	Checklist and Customer Input
Security Requirements	<ul style="list-style-type: none"> <li>Background investigations for 100% of contractor personnel proposed to support task performance shall be favorable.</li> </ul>	<ul style="list-style-type: none"> <li>No violation per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each violation will result in a payment reduction of \$3,600.00 up to the maximum reduction of \$7,200.00.</li> </ul>	Checklist and Customer Input
Personnel Availability	<ul style="list-style-type: none"> <li>100% contractor personnel availability during required daily core hours or specific CLIN required schedules (with the exception of coordinated absences).</li> <li>The contractor is responsible for resource substitution/coverage when a coordinated absence is greater than five consecutive work days.</li> </ul>	<ul style="list-style-type: none"> <li>No violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00.</li> </ul>	



Inquiry Response	<ul style="list-style-type: none"> <li>Respond to all customer inquiries NLT 24 hours after inquiry receipt.</li> </ul>	<ul style="list-style-type: none"> <li>No more than 6 violations per month.</li> <li>A violation is an error (including grammatical errors), omission, or delayed delivery.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of \$2,500.00.</li> </ul>	Checklist and Customer Input
Security Incident Notification and Resolution	<ul style="list-style-type: none"> <li>100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).</li> <li>100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.</li> </ul>	<ul style="list-style-type: none"> <li>No allowable violations per month.</li> </ul>	<ul style="list-style-type: none"> <li>CPARS assessment ratings.</li> <li>In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</li> </ul>	Checklist and Customer Input

Personnel Retention	<ul style="list-style-type: none"> <li>▪ 100% compliance with staffing requirements identified in PWS paragraph 6.4.</li> </ul>	<ul style="list-style-type: none"> <li>▪ No violations per month.</li> <li>▪ No more than 10% personnel turnover (on an individual basis, not positional basis) within an annual performance period.</li> </ul>	<ul style="list-style-type: none"> <li>▪ CPARS assessment ratings.</li> </ul>	Checklist and Customer Input
---------------------	---	---	---	------------------------------